INDEX

COMMUNICATIONS FROM PMSSY SECTION, MOHFW - 2025

SL. NO.	E-MAIL DATED	SUBJECT	PAGE NO.
1.	01.01.2025	O.M. Dated 30.12.2024 regarding "Qualitative Improvements in the Grievance Redressal System of DoHFW of the Ministry of Health & Family Welfare (MoHFW)".	**1-6**
2.	10.01.2025	Letter Dated 09.01.2025 regarding "The theme of the United Nations- International Year of Cooperative UN-IYC-2025 is 'Cooperatives Build a Better Word'- reg."	**7-9**
3.	17.01.2025	Gazette Notification of IB Members.	**10-12**
4.	24.01.2025	Letter Dated 24.01.2025 regarding "PM Surya Ghar: Muft Bijly Yojna- achieving saturation in terms of rooftop solar installation in a time bound manner by December, 2025".	**13-15**
5.	28.01.2025	Office Order Dated 27.01.2025 regarding "Circulation of approved Technical Specifications of Single Plane Digital Subtraction Angiography and Ultrasound machine (Portable/ low end/ high end and premium)".	**16-19**
6.	28.01.2025	Office Order Dated 27.01.2025 regarding "Circulation of approved CT specifications in three different segments (High end 256 slice; Mid end 128 slice and Low end 64 slice)".	**20-87**
7.	29.01.2025	O. M. Dated 21.01.2025 regarding "MoUs/MoCs/Agreements, which are negotiated between Indian institutions and foreign institutions and universities".	**88-115**
8.	29.01.2025	Letter Dated 28.01.2025 regarding "Adherence to Rule 20 of the CCS (Conduct) Rules, 1964 by officers/officials of New AIIMS".	**116-123**
9.	31.01.2025	Letter Dated 31.01.2025 regarding "Request for additional land for expansion of AIIMS".	**124-127**
10.	06.02.2025	Letter Dated 06.02.2024 & Dated 12.12.2024 regarding "Most Immediate: Periodic review of central government employees for strengthening of administration under FR 56 (j) and Rule 48 of CCS (Pension) Rule, 1972 [now, revised as rule of CCS (Pension) Rules, 2021]".	**128-137**
11.	11.02.2025	Office Order Dated 03.02.2025 regarding "Circulation of proposed guidelines for the use of Internal Resources in all new AIIMS/ INIs/Institutes/ Hospitals of the Ministry- seeking comments/suggestions".	**138-161**
12.	20.02.2025	Letter Dated 19.02.2025 regarding "Procedure for reporting, reviewing and accepting of Annual Performance Assessment Reports (APARs) of Financial Advisors in new AIIMS".	**162-165**
13.	24.02.2025	Letter Dated 20.02.2025 regarding "Guidelines concerning identification of posts for persons with benchmark disabilities and their reservation in Central Government Establishments for effective implementation of the RPwD Act, 2016".	**166-175**
14.	03.03.2025	Letter Dated 03.03.2025 with O. M. Dated 27.02.2025 regarding "Procurement and Placement of BHISM Cube at Identified Central Government Hospital/Institutes".	**176-181**

INDEX

COMMUNICATIONS FROM PMSSY SECTION, MoHFW - 2025

SL. NO.	E-MAIL DATED	SUBJECT	PAGE NO.
15.	03.03.2025	O. M. Dated 14.07.2023 regarding "Instructions on Timely submission of Annual Immovable Property Return under Rule 18 (1) of CCS (Conduct) Rules, 1964 by Executive Directors of AIIMS under PMSSY".	**182-189**
16.	04.03.2025	Letter Dated 04.03.2025 regarding "Establishment of dedicated engineering wing to provide technical support and expertise in planning design and execution of sports infrastructure projects".	**190-193**
17.	21.03.2025	O. M. Dated 13.03.2025 regarding "Welfare measures undertaken to secure reservation for the purpose of Article 15(4) and Article 16(4) of the Constitution of India for admission in seat in educational institutions and for appointments or posts in the public services under the control of Ministry of Health and Family Welfare, Government of India for OBCs excluding creamy layer amongst them".	**194-197**
18.	15.04.2025	Letter Dated 15.04.2025 regarding "Conduct of Emergency Medical Technician Diploma Course as in AIIMS Bilaspur".	**198-199**
19.	18.04.2025	Letter Dated 18.04.2025 regarding "Optimal utilization of medical equipment, infrastructure created through CSR and delivery of specialized service- General guidelines".	**200-204**
20.	25.04.2025	Letter Dated 28.04.2025 regarding "Mandatory Security Audit & Certification of Website/Software Applications".	**205-205**
21.	25.04.2025	Letter Dated 28.04.2025 regarding "Undertaking Analysis of Patient Feedback and Implementation of Corrective Measures across all AIIMS".	**206-206**
22.	30.04.2025	Letter Dated 03.04.2025 regarding "Procurement of Medicines and Medical Devices from Hindustan Antibiotic Ltd., Pune".	**207-217**
23.	07.05.2025	Letter Dated 06.05.2025 regarding "Temporary downgrading of post of Financial Advisor (FA) (Pay Level 13) to Senior Accounts Officer (Pay Level 11)".	**218-222**
24.	19.05.2025	Letter Dated 19.05.2025 regarding "Engagement of Retired Faculty on contract basis in new AIIMS".	**223-231**
25.	19.05.2025	Letter Dated 19.05.2025 regarding "Technical Allowance (Tier-I and II) in respect of Defence Personnel appointed on deputation basis in New AIIMS".	**232-234**
26.	21.05.2025	Letter Dated 21.05.2025 regarding "Extension in the period of deputation tenure beyond the initial period of 3 years in new AIIMS".	**235-239**
27.	24.05.2025	O. M. Dated 10.05.2024 regarding "Compliance in respect to the Guidance Framework for Cyber Crises Management Plan".	**240-382**
28.	28.05.2025	Letter Dated 28.05.2025 regarding "Model IT Infra plan for new AIIMS/ INIs".	**383-400**
29.	17.06.2025	Letter Dated 17.06.2025 regarding "Implementation of Swachhata Action Plan (SAP)- 2025-26".	**401-404**

INDEX

COMMUNICATIONS FROM PMSSY SECTION, MOHFW - 2025

SL. NO.	E-MAIL DATED	SUBJECT	PAGE NO.
30.	07.07.2025	Advisory Regarding Cyber Security Audit.	**405-440**
31.	11.07.2025	Cyber Security Advisory received from the National Critical Information Infrastructure Protection Centre (NCIIPC)	**441-512**
32.	16.07.2025	Letter Dated 16.07.2025 regarding "Implementation of SAKSHAM- Learning Management Information System (LMIS) developed by NIHFW".	**513-514**
33.	25.07.2025	Letter Dated 23.07.2025 regarding "Seeking clarification regarding applicability of Reservation Roster for filling up of some posts by promotion at AIIMS, Patna".	**515-517**
34.	29.07.2025	Letter Dated 28.07.2025 regarding "Cyber security guidelines for new AIIMS/INIs".	**518-557**
35.	12.08.2025	Letter Dated 11.08.2025 regarding "Framing of Regulation under the AIIMS Act, 1956 as amended by the Act of 2012".	**558-600**
36.	12.08.2025	O. M. Dated 29.07.2025 regarding "Comprehensive Cyber Security Audit Policy Guidelines"	**601-673**
37.	22.09.2025	Letter Dated 22.09.2025 regarding "Appointment of part-time CVO in new AIIMS".	**674-676**
38.	28.10.2025	Letter Dated 28.10.2025 regarding "Extension in the period of deputation tenure beyond the initial period of 3 years".	**677-706**
39.	17.11.2025	Letter Dated 18.07.2025 regarding "Extension of (a) Transport Allowance at double the normal rates to Persons with Disabilities in accordance with Department of Expenditure's OM Dated 15.09.2022 and (b) Special Allowance for Child Care for Women with Disabilities in accordance with DoPT's instructions dated 18.08.2017".	**707-717**
40.	25.11.2025	Letter Dated 25.11.2025 regarding "Requirement of License issued by CDSCO/State Licensing Authorities in Procurement of Medical Devices by procurement agencies".	**718-720**
41.	25.11.2025	Letter Dated 25.11.2025 regarding "Applicability of DoPT's instructions related to Technical Resignation in new AIIMS".	**721-722**
42.	25.11.2025	Letter Dated 25.11.2025 regarding "Powers for granting administrative approval and financial sanction for incurring expenditure from the Grants-in-aid".	**723-724**
43.	04.12.2025	O. M. Dated 04.12.2025 regarding "Compliance in respect to the information Security Policy for Healthcare (Version 1.0) and security guidelines for consultants and outsourced staff".	**725-751**
44.	05.12.2025	Letter Dated 05.12.2025 regarding "For engagement/appointment of Government counsel from the panel of Union of India for defending Court cases where Union of India is also a party along with an Autonomous Body".	**752-760**
45.	09.12.2025	Letter Dated 09.12.2025 regarding "Preferential procurement of pharmaceutical products manufactured by Goa Antibiotics and Pharmaceuticals Limited (GAPL)".	**761-767**

INDEX

COMMUNICATIONS FROM PMSSY SECTION, MOHFW - 2025

SL. NO.	E-MAIL DATED	SUBJECT	PAGE NO.
46.	09.12.2025	O. M. Dated 03.12.2025 regarding "Compliance of stringent and time-bound directions of Hon'ble Supreme Court of India to all States/UTs and the Union of India regarding a significant rise in dog-bite incidents in institutional spaces".	**768-812**
47.	17.12.2025	Letter Dated 16.12.2025 regarding "Advisory for timely processing of payment of GeM Bills".	**813-815**

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Qualitative improvements in the Grievance Redressal System of DoHFW of the Ministry of Health & Faimly Welfare (MoHFW).

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, Dec 18, 2025 at 11:12 AM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **Ravi Kumar** <ravi.kumar89@gov.in>
Date: Wed, Jan 1, 2025 at 5:07 PM
Subject: Qualitative improvements in the Grievance Redressal System of DoHFW of the Ministry of Health & Faimly Welfare (MoHFW).
To: director <director@aiimsbhopal.edu.in>, director <director@aiimsbhubaneswar.edu.in>, director <director@aiimsjodhpur.edu.in>, director <director@aiimspatna.org>, director <director@aiimsraipur.edu.in>, director <director@aiimsrishikesh.edu.in>, edaiimsrbl <edaiimsrbl@gmail.com>, rajwanshiarvind <rajwanshiarvind@hotmail.com>, director <director@aiimsmangalagiri.edu.in>, directoraiimsnagpur <directoraiimsnagpur@gmail.com>, sramji57 <sramji57@gmail.com>, executivedirector <executivedirector@aiimsgorakhpur.edu.in>, director <director@aiimsbathinda.in>, director <director@aiimsdeoghar.edu.in>, director <director@aiimsbibinagar.edu.in>, vsnegi22 <vsnegi22@yahoo.co.in>, shakti810505 <shakti810505@gmail.com>, drmhraosvims1957 <drmhraosvims1957@gmai.com>, cdskatoch <cdskatoch@gmail.com>, puranik_6 <puranik_6@hotmail.com>, madhabananda <madhabananda@gmail.com>, director <director@aiimsguwahati.ac.in>, director <director@aiimsbilaspur.edu.in>, ed <ed@aiimskalyani.edu.in>, director <director@jipmer.edu.in>, edaiimsrajkot <ed.aiimsrajkot@gmail.com>, ddaaiimsawantipora1 <ddaaiimsawantipora1@gmail.com>, sachimohanty <sachimohanty@rediffmail.com>, dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, Manumanish Gupta <guptairss@gmail.com>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, Saroj Singh <sarojkr.singh@gov.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, Dr. PRADIP KUMAR <kpradip10@gmail.com>, kochas27 <kochas27@gmail.com>, Rajeev Sen Roy <rajeevsenroy30@gmail.com>, dda <dda@aiimsbathinda.edu.in>, AMRENDRA KUMAR <amrendra.kumar72@gov.in>, officeaiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda <dda@aiimsdeoghar.edu.in>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, ddaaiimsbilaspur <ddaaiimsbilaspur@gmail.com>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, thaiumag <thaiu.mag@gov.in>, dda <dda@aiimskalyani.edu.in>, dda <dda@aiimsgorakhpur.edu.in>
Cc: Shri Secretary <raj.kumar28@nic.in>, Mayukh Ranjan Paul <mayukh.paul88@gov.in>, Anshuli Chauhan <anshuli.tandon@gov.in>, GUNJANSHARMA <gunjan.s@gov.in>, bme pmssy <bme.pmssy@yahoo.com>

Respected Madam/Sir,

W.r.t. the subject above, kindly find the enclosed **Office Memorandum** letter No F.No-13016/08/2024-W&PG dated 30.12.2024, for further necessary action.
With regards.

Section Officer(PMSSY-I)

MoHFW

OM Dated 30.12.2024.pdf
463K

4020571

PRIORITY

F. No. B-13016/08/2024-W&PG
Government of India
Ministry of Health and Family Welfare
(W&PG Section)

Nirman Bhawan, New Delhi-110011
Dated 30th December, 2024

OFFICE MEMORANDUM

Subject: Qualitative improvements in the Grievance Redressal System of DoHFW of the Ministry of Health & Family Welfare (MoHFW).

The undersigned is directed to inform that a review meeting, under the Chairmanship of Advisor to Hon'ble Prime Minister, was held on 20.12.2024 in Prime Minister's Office and, during the course of meeting, it was desired that the Ministry should make qualitative improvements in its Grievance Redressal System to make it more sensitive, accessible and meaningful.

2. In this connection, the following action points have been decided:

(i) 20 cases *(received on the **CPGRAMS** portal)* will be randomly reviewed by Secretary (HFW) in a month.

(ii) All Sub-Appellate Authorities (SAAs) of CPGRAMS are required to review 10 cases monthly, **by calling the complainants**, where 'Poor' feedback has been received from the complainants on the portal.

(iii) Each Division should carry out **Root Cause Analysis**' of Public Grievances received in the Division to identify areas of concerns as well as requirement of any systemic reforms and should take necessary action.

(iv) Further, **Head of the Institutions** should review 20-50 cases monthly and the report of the same should be submitted to the concerned Divisions Heads in MoHFW.

3. Action taken on the points mentioned above will be reviewed by Secretary (HFW) every 2nd week of the month. **All are, therefore, requested to take necessary action for compliance of aforesaid directions.**

Signed by
Jitender Singh (Jitender Singh)
Deputy Secretary to the Government of India &
Nodal Grievance Redressal Officer
Date: 30-12-2024 17:04:42
Tele No. 011-23062292

Please also circulate it to all AIIMS & INIs.

To
(through e-Office's Notice Board)

01/01/25

Dir(INI)/ Dir(Misc)/ Dir(PCP)/ JD(DK)/ DS(KK)/ DS(AT)

1/1 SO(PMSSY-I)

(i) AS(RS)/ AS(LSC)/ AS(VHZ)/ AS&MD(NHM)

(ii) JS(PR)/ JS(AMB)/ JS(SJ)/ JS(MK)/ JS(VJ)/ JS(ERS)/ JS(LG)/ JS(NG)/ JS(MKB)/ JS(MS)/ JS(GM) of Dte.GHS/ Sr EA(IK)/ EA(KKT)/ CCA/ Adv (RW)

(iii) All Directors/ Deputy Secretaries/ Joint Directors and equivalent officers (who are Grievance Redressal Officers on CPGRAMS)

Copy to (for information):
PSO to Secretary (HFW)

4020571

PRIORITY

F. No. B-13016/08/2024-W&PG
Government of India
Ministry of Health and Family Welfare
(W&PG Section)

Nirman Bhawan, New Delhi-110011
Dated 30th December, 2024

OFFICE MEMORANDUM

Subject: Qualitative improvements in the Grievance Redressal System of DoHFW of the Ministry of Health & Family Welfare (MoHFW).

The undersigned is directed to inform that a review meeting, under the Chairmanship of Advisor to Hon'ble Prime Minister, was held on 20.12.2024 in Prime Minister's Office and, during the course of meeting, it was desired that the Ministry should make qualitative improvements in its Grievance Redressal System to make it more sensitive, accessible and meaningful.

2. In this connection, the following action points have been decided:

(i) 20 cases *(received on the **CPGRAMS** portal)* will be randomly reviewed by Secretary (HFW) in a month.

(ii) All Sub-Appellate Authorities (SAAs) of CPGRAMS are required to review 10 cases monthly, **by calling the complainants**, where **'Poor'** feedback has been received from the complainants on the portal.

(iii) Each Division should carry out **Root Cause Analysis'** of Public Grievances received in the Division to identify areas of concerns as well as requirement of any systemic reforms and should take necessary action.

(iv) Further, **Head of the Institutions** should review 20-50 cases monthly and the report of the same should be submitted to the concerned Divisions Heads in MoHFW.

3. Action taken on the points mentioned above will be reviewed by Secretary (HFW) every 2nd week of the month. **All are, therefore, requested to take necessary action for compliance of aforesaid directions.**

Signed by
Jitender Singh (Jitender Singh)
Deputy Secretary to the Government of India &
Nodal Grievance Redressal Officer
Tele No. 011-23062292
Date: 30-12-2024 17:04:42

Please also circulate it to all AIIMS & INIs.

To
(through e-Office's Notice Board)

01/01/25

Dir(INI) / Dir(MI&O) / Dir(PCP) / JD(DK) / DS(KK) / DS(AT)

1/1
SO(MMS-I)

(i) AS(RS)/ AS(LSC)/ AS(VHZ)/ AS&MD(NHM)

(ii) JS(PR)/ JS(AMB)/ JS(SJ)/ JS(MK)/ JS(VJ)/ JS(ERS)/ JS(LG)/ JS(NG)/ JS(MKB)/ JS(MS)/ JS(GM) of Dte.GHS/ Sr EA(IK)/ EA(KKT)/ CCA/ Adv (RW)

(iii) All Directors/ Deputy Secretaries/ Joint Directors and equivalent officers (who are Grievance Redressal Officers on CPGRAMS)

Copy to (for information):
PSO to Secretary (HFW)

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: The theme of the United Nations - International Year of Cooperative UN-IYC-2025 is "Cooperatives Build a Better World"- reg.

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, Dec 18, 2025 at 11:08 AM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **Director .** <director@aiimspatna.org>
Date: Fri, Jan 10, 2025 at 11:45 AM
Subject: Fwd: The theme of the United Nations - International Year of Cooperative UN-IYC-2025 is "Cooperatives Build a Better World"- reg.
To: DDA AIIMS PATNA <dda@aiimspatna.org>
Cc: SAURABH VARSHNEY <drsaurabh68@gmail.com>

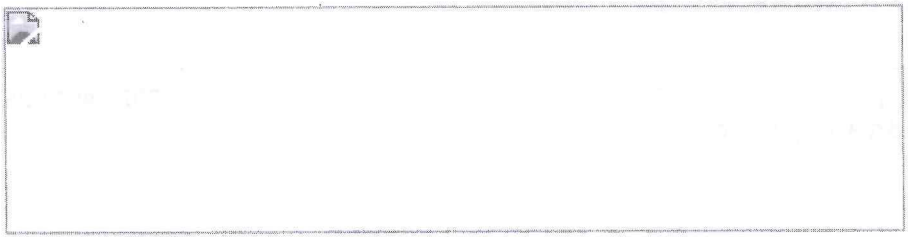
Sd/-
Prof. (Dr.) Saurabh Varshney
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109

---------- Forwarded message ---------
From: **Mr Sourabh** <pmssy5-mohfw@gov.in>
Date: Fri, Jan 10, 2025 at 10:14 AM
Subject: The theme of the United Nations - International Year of Cooperative UN-IYC-2025 is "Cooperatives Build a Better World"- reg.
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Executive Director Raebareli <ed.aiimsrbl@gmail.com>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, Dinesh Singh <director@aiimsbathinda.edu.in>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, Director AIIMS Madurai <drmhraosvims1957@gmail.com>, ED AIIMS Guwahati <executive-director@aiimsguwahati.ac.in>, ED AIIMS Bilaspur <edaiimsbls@gmail.com>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Director AIIMS Vijaypur <shakti810505@gmail.com>, DDA AIIMS Awantipora <rakeshkumar7123@yahoo.in>, Executive Director AIIMS Rajkot <ed.aiimsrajkot@gmail.com>, Director AIIMS Bibinagar <director.aiimsbbnagar@gmail.com>, Executive Director AIIMS Darbhanga <madhabananda@gmail.com>
Cc: DEEPAK KUMAR BHATT <healthcdn-mohfw@gov.in>, Phool Chandra Prasad <prasad-upsc@gov.in>, Dharm Bir Kumar SIngh <dharmbk.singh@nic.in>, Sourabh <sourabh.12@gov.in>

Respected Sir/Madam,

With reference to the subject cited above, Please find the attachment herewith.

Regards
PMSSY-V Section
Ministry of Health and Family Welfare



2 attachments

Letter dated 09-01-2025.pdf
88K

Encl__ (.pdf
1151K

File No.: Z-28015/01/2025-PMSSY-V (FTS: 8314406)
Government of India
Ministry of Health & Family Welfare
(Department of Health & Family Welfare)
(PMSSY-V Section)

Nirman Bhawan, New Delhi-110011.
Dated: 09-01-2025

To
Executive Director,
[All AIIMS under PMSSY Division].

Subject: The theme of the United Nations - International Year of Cooperative UN-IYC-2025 is "Cooperatives Build a Better World"- reg.

Sir,

I am directed to refer to this Ministry's OM No. Z.28020/76/2023-CDN dated 06.01.2025(copy enclosed) & DO No. A-58011/2/2024-MoC dated 26.12.2024 from Secretary, Ministry of Cooperation(copy enclosed) regarding the subject mentioned above and to say that United Nations has declared the Year 2025 as International Year of Cooperative (UN- IYC-2025) with the theme "Cooperatives Build a Better World", underscoring the transformative role cooperatives play in promoting social inclusion, economic empowerment, and sustainable development.

2. This was officially launched in India by the Hon'ble Prime Minister in the International Cooperative Alliance (ICA) Global Conference held recently at Bharat Mandapam New Delhi. Therefore, to commemorate this zeal and promote it across the country, you are requested to use the Logo (copy enclosed) of UN-IYC -2025 on website, portals, stationery items, events and prominent places in the premises.

Yours faithfully,

Digitally signed by
Dharm Bir Kumar Singh
Date: 09-01-2025
17:10:58

(Dharm Bir Kumar Singh)
(Under Secretary to the Government of India)
Tele: 011-23060006

Enc: as above.

Copy for information to:

Under Secretary, Coordination Division, DoH&FW, Nirman Bhawan, New Delhi.

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Gazette notification of IB members- reg

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, Dec 18, 2025 at 11:07 AM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **pmssysection iv** <pmssysectioniv@gmail.com>
Date: Fri, Jan 17, 2025 at 3:41 PM
Subject: Gazette notification of IB members- reg
To: Director Patna <director@aiimspatna.org>, DDA AIIMS PATNA <dda@aiimspatna.org>
Cc: Cc: <Dinesh.kumar14@nic.in>, : <Ak.biswas57@nic.in>, Mr.SankarGarg Mr.SankarGarg <sankar.garg@gov.in>, Amit Batra <amit.batra@gov.in>

Sir/ Madam,

Please find the attachment, for further necessary action.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officials of PMSSY-IV Section at - dinesh.kumar14@nic.in; ak. biswas57@nic.in; sankar.garg@gov.in; amit.batra@gov.in

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

15,16 - 13.01.2025 - 257 - 14.01.2025.pdf
425K

रजिस्ट्री सं. डी.एल.- 33004/99 REGD. No. D. L.-33004/99

सत्यमेव जयते

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-15012025-260240
CG-DL-E-15012025-260240

असाधारण
EXTRAORDINARY

भाग II—खण्ड 3—उप-खण्ड (ii)
PART II—Section 3—Sub-section (ii)

प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 255] नई दिल्ली, मंगलवार, जनवरी 14, 2025/पौष 24, 1946
No. 255] NEW DELHI, TUESDAY, JANUARY 14, 2025/PAUSHA 24, 1946

स्वास्थ्य एवं परिवार कल्याण मंत्रालय

अधिसूचना

नई दिल्ली, 13 जनवरी, 2025

का.आ. 257(अ).—केंद्र सरकार, अखिल भारतीय आयुर्विज्ञान संस्थान (संशोधन) अधिनियम, 2012 (2012 का 37) द्वारा यथा संशोधित अखिल भारतीय आयुर्विज्ञान संस्थान अधिनियम, 1956 (1956 का 25) की धारा 4 (छ) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए, लोक सभा के सदस्यों द्वारा निर्वाचित, **श्री तारिक अनवर** और **श्री रवि शंकर प्रसाद** को अखिल भारतीय आयुर्विज्ञान संस्थान, **पटना** के संस्थान निकाय के सदस्यों के रूप में कार्य करने के लिए अधिसूचित करती है।

सदस्यगण का कार्यकाल अखिल भारतीय आयुर्विज्ञान संस्थान अधिनियम, 1956 की धारा 6 में निहित प्रावधानों द्वारा शासित होगा।

[फा. सं. जेड-28016/177/2019-पीएमएसएसवाई.IV(भाग-1)(8046724)]

अंकिता मिश्रा बुंदेला, संयुक्त सचिव

MINISTRY OF HEALTH AND FAMILY WELFARE

NOTIFICATION

New Delhi, the 13th January, 2025

S.O. 257(E).—In exercise of powers conferred by Section 4(g) of the All India Institute of Medical Sciences Act, 1956 (25 of 1956) as amended by All India Institute of Medical Sciences (Amendment) Act, 2012 (37 of 2012), the Central Government hereby notifies **Shri Tariq Anwar** and **Shri Ravi Shankar Prasad**, elected by the Members of Lok Sabha to serve as Members of the Institute Body of All India Institute of Medical Sciences, **Patna.**

The term of office of members shall be governed by the provisions contained in Section 6 of the All India Institute of Medical Sciences Act, 1956.

[F. No. Z-28016/177/2019-PMSSY.IV-Part(1)(8046724)]

ANKITA MISHRA BUNDELA, Jt. Secy.

Uploaded by Dte. of Printing at Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.

GORAKHA NATH YADAVA Digitally signed by GORAKHA NATH YADAVA Date: 2025.01.15 12:27:10 +05'30'

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: PM Surya Ghar: Muft Bijli Yojna - achieving saturation in terms of rooftop solar installation in a time bound manner by Dec. 2025.

2 messages

Director . <director@aiimspatna.org> Mon, Feb 3, 2025 at 12:53 PM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Sd/-
Prof. (Dr.) Saurabh Varshney
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109

---------- Forwarded message ---------
From: **Mr Sourabh** <pmssy5-mohfw@gov.in>
Date: Fri, Jan 24, 2025 at 12:52 PM
Subject: PM Surya Ghar: Muft Bijli Yojna - achieving saturation in terms of rooftop solar installation in a time bound manner by Dec. 2025.
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Executive Director Raebareli <ed.aiimsrbl@gmail.com>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, Dinesh Singh <director@aiimsbathinda.edu.in>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, Director AIIMS Madurai <drmhraosvims1957@gmail.com>, ED AIIMS Guwahati <executive-director@aiimsguwahati.ac.in>, ED AIIMS Bilaspur <edaiimsbls@gmail.com>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Director AIIMS Vijaypur <shakti810505@gmail.com>, DDA AIIMS Awantipora <rakeshkumar7123@yahoo.in>, Executive Director AIIMS Rajkot <ed.aiimsrajkot@gmail.com>, Director AIIMS Bibinagar <director.aiimsbbnagar@gmail.com>, Executive Director AIIMS Darbhanga <madhabananda@gmail.com>
Cc: <ravi.ranjan@aiimspatna.org>, <dda@aiimsbilaspur.edu.in>, <eeel@aiimsbhubaneswar.edu.in>, <bhandarih@aiimsjodhpur.edu.in>, <prakharje.elect@aiimsbhopal.edu.in>, <se@aiimsmangalagiri.edu.in>, <dda@aiimsguwahati.ac.in>, <se@aiimsgorakhpur.edu.in>, <estatebranch@aiimsbathinda.in>, <se@aiimsnagpur.edu.in>, <yogisclass1@gmail.com>, <eee@aiimsrishikesh.edu.in>, <se@aiimsraipur.edu.in>, <se@aiimskalyani.edu.in>, <Engg.dept.aiimsrajkot@gmail.com>, Govardhana D <supdt.engg@aiimsbibinagar.edu.in>, <jairam.gajar@aiimsjammu.edu.in>, <engineering@aiimsdeoghar.edu.in>, <ddaaiimsawatipora1@gmail.com>, DDA BHOPAL <dydir@aiimsbhopal.edu.in>, DDA Bhubaneswar <dda@aiimsbhubaneswar.edu.in>, DDA Jodhpur <dda@aiimsjodhpur.edu.in>, DDA AIIMS Patna <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, DDA AIIMS Rishikesh <dda@aiimsrishikesh.edu.in>, DDA RAEBARELI <ddaaiimsrbl@gmail.com>, DDA NAGPUR <dda@aiimsnagpur.edu.in>, Dr. DDA AIIMS Kalyani <kpradip10@gmail.com>, dda bilaspur <ddaaiimsbilaspur@gmail.com>, DDA AIIMS Deoghar AIIMS Deoghar <dda@aiimsdeoghar.edu.in>, AMRENDRA KUMAR <amrendra.kumar72@gov.in>, DDA AIIMS Madurai <ddamadurai1189@gmail.com>, DDA AIIMS Rajkot <dda.aiimsrajkot@gmail.com>, DDA AIIMS BIBINAGAR <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Vijaypur, Jammu <ddaaiimsjammu@gmail.com>, Phool Chandra Prasad <prasad-upsc@gov.in>, Dharm Bir Kumar SIngh <dharmbk.singh@nic.in>, Sourabh <sourabh.12@gov.in>, AIIMS DDA Gorakhpur <dda@aiimsgorakhpur.edu.in>, DDA AIIMS Bathinda <rajeevsenroy30@gmail.com>

Respected Sir/Madam,

With reference to the subject cited above, please find the attachment.

Regards
PMSSY-V Section
Ministry of Health and Family Welfare

13



3 attachments

Letter dated 24-01-25.pdf
90K

Updated Rooftop format (as on01.01.2025).xlsx
17K

PM Surya Ghar Note-Secy (1).pdf
1785K

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, Dec 18, 2025 at 11:00 AM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507
[Quoted text hidden]

3 attachments

Letter dated 24-01-25.pdf
90K

Updated Rooftop format (as on01.01.2025).xlsx
17K

PM Surya Ghar Note-Secy (1).pdf
1785K

Digitally signed copy

Z-28016/170/2024-PMSSY-V[8291083]
Government of India
Ministry of Health and Family Welfare
(PMSSY - V Section)
Nirman Bhawan, New Delhi-110011
Dated the24-01-2025

To
The Executive Director
[All AIIMS under PMSSY Division]

Subject: PM Surya Ghar: Muft Bijli Yojna - achieving saturation in terms of rooftop solar installation in a time bound manner by Dec. 2025

Sir/ Madam,

I am directed to forward herewith a copy of Secretary, HFW Note No.Z-17022/13/2020-BP dated 16.01.2025 (copy enclosed) on the subject mentioned above and to say that under PM Surya Ghar : Muft Bijli Yojana, to achieve saturation in terms of rooftop solar installation in a time bound manner by Dec' 2025 for which a Steering Committee headed by Cabinet Secretary has also been set up to monitor the progress, the following activities are imperative:

i. **Baseline assessment** of potential rooftop solar capacity based on availability of appropriate roof space
ii. **Gap assessment** viz. solar capacity already installed and
iii. Make a **time bound action plan** to fill the gap to achieve the saturation by end 2025.

2. Further, for achieving saturation, NTPC, Vidyut Vyapar Nigam Limited (NNVN) has been designated as the Nodal Agency to assist in the development solar rooftop projects either on Capex mode or RESCO mode. A workshop is also being organized by NNVN and BoP jointly to familiarize the Heads of Institutions of the steps and roles/responsibilities in this joint endeavour to achieve saturation, details of which will be shared with the Institutes.

3. Accordingly, all the institutions are advised to review the data shared by them to this Ministry and to **identify feasible surface area** for Solar RTS, **resolve bottlenecks, if any** and **prioritize preparation and achievement of time bound plan for achieving solar saturation** of Government Buildings and submit updated status to this Ministry for review of the progress, latest by 30th January, 2025. A copy of the details /data shared by the institutes on the said matter is also enclosed for reference.

Yours faithfully,
Digitally signed by
Dharm Bir Kumar Singh
Date: 24-01-2025
11:07:44
(Dharm Bir Kumar Singh)
Under Secretary to the Govt. of India

Copy to:

1. DDAs , All AIIMS under PMSSY.
2. Nodal Officers of AIIMS identified under PM Surya Ghar - reg.

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Circulation of approved Technical Specifications of Single Plane Digital Subtraction Angiography and Ultrasound machine (Portable/ low end/ high end and premium) – reg.

2 messages

Director . <director@aiimspatna.org> Mon, Feb 3, 2025 at 12:52 PM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Sd/-
Prof. (Dr.) Saurabh Varshney
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109

---------- Forwarded message ---------
From: **pmssysection iv** <pmssysectioniv@gmail.com>
Date: Tue, Jan 28, 2025 at 11:52 AM
Subject: Circulation of approved Technical Specifications of Single Plane Digital Subtraction Angiography and Ultrasound machine (Portable/ low end/ high end and premium) – reg.
To: Jaideep Kumar Mishra <asfa-mhfw@nic.in>, <Laxmi.narayan27@nic.in>, <vinod.kumar38@nic.in>, Roli Singh <roli.singh@ias.nic.in>, Roli Singh <ash-mohfw@nic.in>, ROLI SINGH <asfr-mohfw@gov.in>, <Veena.sethi@nic.in>, <pc.mardi@nic.in>, <oo.asphp-mohfw@gov.in>, Ms. V Hekali Zhimomi <zhimomiv@ias.nic.in>, Ms. V. Hekali Zhimomi <dgoffice@naco.gov.in>, <d.jeevaraj38@nic.in>, Aradhana Patnaik <asmd-mohfw@nic.in>, <jsehealth-mohfw@gov.in>, <harish.jain68@nic.in>, <js.me-mohfw@nic.in>, ANKITA MISHRA BUNDELA <js-pmssy-mohfw@gov.in>, <js.policy-mohfw@gov.in>, Praveen Batra <Praveen.batra@gov.in>, <sk.karwal@gov.in>, Vandana Jain <vandana.jain@nic.in>, <mukesh.khetan@nic.in>, Dr. Manashvi kumar <jstraining-mohfw@gov.in>, Elangbam Robert Singh <robert.elangbam@gov.in>, <kuldeep.saini69@nic.in>, <g.latha@nic.in>, Vijay Kumar Sinha <sinha.vijay@nic.in>, <raminder.rana70@nic.in>, Indrani Kaushal <ea-mohfw@nic.in>, <indrani.k@nic.in>, Dr. K. K. Tripathy <kk.tripathy@nic.in>, RAJIV WADHAWAN <r.wadhawan15@nic.in>, <ashutosh.72@nic.in>, Ms Meera Srivastava <jsrch-mohfw@gov.in>, <shammi.chhabra@nic.in>, <nikhil.g@ias.nic.in>, Smt. Jaspal Kaur <cca-mohfw@nic.in>, <jai.shree27@gov.in>, Anoop Kumar Puri <anoopk.puri@nic.in>, j_mishra <j_mishra@gov.in>, L Sweety Changsan <lschangsan@nic.in>, Pushpendra Rajput <Pushpendra.r@nic.in>, <Ddgtb@rntcp.org>, Pradeep Khasnobis <pradeep.khasnobis@gov.in>, Saurabh Jain <js-publichealth@gov.in>, ANKITA MISHRA BUNDELA <Ankita.edu@nic.in>, Prof (Dr) Atul Goel <dghs@nic.in>
Cc: Srinivas.M <director@aiims.gov.in>, <director@jipmer.ac.in>, Varun Ahluwalia <ahluwaliav@cag.gov.in>, Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, Executive Director Raebareli <edaiimsrbl@gmail.com>, <rajwanshiarvind@hotmail.com>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, <madhabananda@gmail.com>, <sachimohanty@rediffmail.in>, <ceo@hllhites.com>, Apurva Chandra <secyhfw@nic.in>, Cc: <Dinesh.kumar14@nic.in>, NIMHANS <dirstaff@nimhans.ac.in>, MS OFFICE SJH <msoffice@vmmc-sjh.nic.in>, Dr. Sunita Sharma <director-lhmc@gov.in>, minakshi Bhardwaj <med.sup@rmlh.nic.in>, : <Ak.biswas57@nic.in>, Mr.SankarGarg Mr.SankarGarg <sankar.garg@gov.in>, Amit Batra <amit.batra@gov.in>, Prof. Dr. D.K. Singh, Director <director@aiimsbathinda.in>, Executive Director AIIMS Rajkot <ed.aiimsrajkot@gmail.com>, Dr Vivek Lal <dpgi@pgimer.edu.in>, Director Neigrihms <director-neigrihms@gov.in>, <nalinaiims.mehta@gmail.com>, <eigasunil@gmail.com>, <director@ripans.ac.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officials of PMSSY-IV Section at - dinesh.kumar14@nic.in; ak.biswas57@nic.in; sankar.garg@gov.in; amit.batra@gov.in

Regards
PMSSY-IV Section

ENCL (18).pdf

Ministry of Health and Family Welfare

2 attachments

Letter (68).pdf
92K

Circulation of approved Technical Specifications of 10 Medical equipment.pdf
18402K

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, Dec 18, 2025 at 10:58 AM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507
[Quoted text hidden]

2 attachments

Letter (68).pdf
92K

Circulation of approved Technical Specifications of 10 Medical equipment.pdf
18402K

Z-28016/35/2024-PMSSY-IV(8285627)
Government of India
Ministry of Health & Family Welfare
(PMSSY-IV Section)

Room No. 745-A, Nirman Bhawan, New Delhi
Dated the 27-01-2025

Office Order

Subject: Circulation of approved Technical Specifications of Single Plane Digital Subtraction Angiography and Ultrasound machine (Portable/ low end/ high end and premium) – reg.

In continuation of the office order of even no dated 21.08.2024, please find enclosed herewith the Technical Specifications of Single Plane Digital Subtraction Angiography and Ultrasound machine (Portable/ low end/ high end and premium) as submitted by the Committee set up by MoHFW under the Chairpersonship of Dr. Raju Sharma, Professor & Head, Department of Radiodiagnosis & Interventional Radiology, AIIMS New Delhi.

2. The above specifications have the approval of Secretary (HFW) and shall be valid for two years. All AIIMS/ INIs/ Institutes/ Hospitals/ Procurement Support Agency (HITES) of the Ministry are advised to adhere to the approved specifications (enclosed) while undertaking procurement of these equipment.

Digitally signed by
ARUN KUMAR BISWAS
Date: 27-01-2025
13:01:27

(Arun Kumar Biswas)
Under Secretary to the Govt. of India
Tel:011-23061343

Encl(2):

i. Technical Specifications of Single Plane Digital Subtraction Angiography and Ultrasound machine (Portable/ low end/ high end and premium)
ii. office order of even no dated 21.08.2024

To

i. All Additional Secretaries/ Joint Secretaries, MoHFW – with a request to circulate the proposed Guidelines to all the Institutes/ Hospitals/ Autonomous Bodies under their administrative control.

ii. Director General of Health Services, MoHFW, GoI

Copy to :

i. Director, AIIMS New Delhi

ii. Director, PGIMER, Chandigarh,

iii. Director, JIPMER, Puducherry

iv. Director, NIMHNAS, Bengaluru

v. The Directors/ Executive Directors of new AIIMS under PMSSY

vi. The Directors of Central Government Hospitals in Delhi/ North East Hospitals

vii. CEO, HITES (via email at ceo@hllhites.com)

Copy for information to :

i. PSO to Secretary(HFW)

ii. PPS to Joint Secretary (PMSSY)

iii. PS Director (PMSSY-IV)

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Circulation of approved CT specifications in three different segments (High end 256 slice; Mid end 128 slice and Low end 64 slice)– reg.

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, Dec 18, 2025 at 11:05 AM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **Director .** <director@aiimspatna.org>
Date: Tue, Jan 28, 2025 at 1:42 PM
Subject: Fwd: Circulation of approved CT specifications in three different segments (High end 256 slice; Mid end 128 slice and Low end 64 slice)– reg.
To: medical superitendent <ms@aiimspatna.org>, MS Office <mso@aiimspatna.org>, Radiodiagnosis Dept <radiodiagnosis@aiimspatna.org>, Procurement AIIMSPatna <procurement@aiimspatna.org>, Dr Binod Kumar Pati <drbinodkumarpati@aiimspatna.org>, DDA AIIMS PATNA <dda@aiimspatna.org>

Sd/-
Prof. (Dr.) Saurabh Varshney
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109

---------- Forwarded message ---------
From: **pmssysection iv** <pmssysectioniv@gmail.com>
Date: Tue, Jan 28, 2025 at 10:18 AM
Subject: Circulation of approved CT specifications in three different segments (High end 256 slice; Mid end 128 slice and Low end 64 slice)– reg.
To: Jaideep Kumar Mishra <asfa-mhfw@nic.in>, <Laxmi.narayan27@nic.in>, <vinod.kumar38@nic.in>, Roli Singh <roli.singh@ias.nic.in>, Roli Singh <ash-mohfw@nic.in>, ROLI SINGH <asfr-mohfw@gov.in>, <Veena.sethi@nic.in>, <pc.mardi@nic.in>, <oo.asphp-mohfw@gov.in>, Ms. V Hekali Zhimomi <zhimomiv@ias.nic.in>, Ms. V. Hekali Zhimomi <dgoffice@naco.gov.in>, <d.jeevaraj38@nic.in>, Aradhana Patnaik <asmd-mohfw@nic.in>, <jsehealth-mohfw@gov.in>, ANKITA MISHRA BUNDELA <js-pmssy-mohfw@gov.in>, <js.policy-mohfw@gov.in>, Praveen Batra <Praveen.batra@gov.in>, <sk.karwal@gov.in>, Vandana Jain <vandana.jain@nic.in>, <mukesh.khetan@nic.in>, Dr. Manashvi kumar <jstraining-mohfw@gov.in>, Elangbam Robert Singh <robert.elangbam@gov.in>, <kuldeep.saini69@nic.in>, <g.latha@nic.in>, Vijay Kumar Sinha <sinha.vijay@nic.in>, <raminder.rana70@nic.in>, Indrani Kaushal <ea-mohfw@nic.in>, <indrani.k@nic.in>, Dr. K. K. Tripathy <kk.tripathy@nic.in>, RAJIV WADHAWAN <r.wadhawan15@nic.in>, <ashutosh.72@nic.in>, Ms Meera Srivastava <jsrch-mohfw@gov.in>, <shammi.chhabra@nic.in>, <nikhil.g@ias.nic.in>, Smt. Jaspal Kaur <cca-mohfw@nic.in>, <jai.shree27@gov.in>, Anoop Kumar Puri <anoopk.puri@nic.in>, j_mishra <j_mishra@gov.in>, L Sweety Changsan <lschangsan@nic.in>, Pushpendra Rajput <Pushpendra.r@nic.in>, <Ddgtb@rntcp.org>, Pradeep Khasnobis <pradeep.khasnobis@gov.in>, Saurabh Jain <js-publichealth@gov.in>, ANKITA MISHRA BUNDELA <Ankita.edu@nic.in>, Prof (Dr) Atul Goel <dghs@nic.in>
Cc: Srinivas.M <director@aiims.gov.in>, <director@jipmer.ac.in>, Varun Ahluwalia <ahluwaliav@cag.gov.in>, Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director

AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, Executive Director Raebareli <edaiimsrbl@gmail.com>, <rajwanshiarvind@hotmail.com>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, <madhabananda@gmail.com>, <sachimohanty@rediffmail.in>, <ceo@hllhites.com>, Apurva Chandra <secyhfw@nic.in>, Cc: <Dinesh.kumar14@nic.in>, NIMHANS <dirstaff@nimhans.ac.in>, MS OFFICE SJH <msoffice@vmmc-sjh.nic.in>, Dr. Sunita Sharma <director-lhmc@gov.in>, minakshi Bhardwaj <med.sup@rmlh.nic.in>, : <Ak.biswas57@nic.in>, Mr.SankarGarg Mr.SankarGarg <sankar.garg@gov.in>, Amit Batra <amit.batra@gov.in>, Prof. Dr. D.K. Singh, Director <director@aiimsbathinda.in>, Executive Director AIIMS Rajkot <ed.aiimsrajkot@gmail.com>, Dr Vivek Lal <dpgi@pgimer.edu.in>, Director Neigrihms <director-neigrihms@gov.in>, <nalinaiims.mehta@gmail.com>, <eigasunil@gmail.com>, <director@ripans.ac.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officials of PMSSY-IV Section at - dinesh.kumar14@nic.in; ak.biswas57@nic.in; sankar.garg@gov.in; amit.batra@gov.in

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

---

3 attachments

Office Order (10).pdf
98K

ENCL (17).pdf
599K

Circulation of approved Technical Specifications of 10 Medical equipment.pdf
18402K

Z-28016/35/2024-PMSSY-IV-Part(3)(8310053)
Government of India
Ministry of Health & Family Welfare
(PMSSY-IV Section)

Room No. 745-A, Nirman Bhawan, New Delhi

Dated the 27-01-2025

Office Order

Subject: Circulation of approved CT specifications in three different segments (High end 256 slice; Mid end 128 slice and Low end 64 slice)– reg.

In continuation of the office order of even no dated 21.08.2024, please find enclosed herewith specifications of CT Scan machine in three different segments (High end 256 slice; Mid end 128 slice and Low end 64 slice) as submitted by the Committee set up by MoHFW under the Chairpersonship of Dr. Raju Sharma, Professor & Head, Department of Radiodiagnosis & Interventional Radiology, AIIMS New Delhi.

2. The above specifications have the approval of Secretary (HFW) and shall be valid for two years. All AIIMS/ INIs/ Institutes/ Hospitals/ Procurement Support Agency (HITES) of the Ministry are advised to adhere to the approved specifications (enclosed) while undertaking procurement of these equipment.

Digitally signed by
ARUN KUMAR BISWAS
Date: 27-01-2025
16:06:00

(Arun Kumar Biswas)
Under Secretary to the Govt. of India
Tel:011-23061343

Encl(2):

i. Specifications of CT Scan Machine in three different segments (High end 256 slice; Mid end 128 slice and Low end 64 slice)

ii. Office order of even no dated 21.08.2024

To

i. All Additional Secretaries/ Joint Secretaries, MoHFW – with a request to circulate the proposed Guidelines to all the Institutes/ Hospitals/ Autonomous Bodies under their administrative control.

ii. Director General of Health Services, MoHFW, GoI

Copy to :

i. Director, AIIMS New Delhi

ii. Director, PGIMER, Chandigarh,

iii. Director, JIPMER, Puducherry

iv. Director, NIMHNAS, Bengaluru

v. The Directors/ Executive Directors of new AIIMS under PMSSY

vi. The Directors of Central Government Hospitals in Delhi/ North East Hospitals

vii. CEO, HITES (via email at ceo@hllhites.com)

Copy for information to :

i. PSO to Secretary(HFW)

ii. PPS to Joint Secretary (PMSSY)

iii. PS Director (PMSSY-IV)

Fwd: CT specifications: 3 different segments

DK Dinesh Kumar <dinesh.kumar14@nic.in>
Mon, 09 Dec 2024 12:45:15 PM +0530

To "ARUN BISWAS" <ak.biswas57@nic.in>, "SANKAR GARG" <sankar.garg@gov.in>, "Amit Batra" <amit.batra@gov.in>

Please put up today

========== Forwarded message ==========
From: ANKITA MISHRA BUNDELA <js-pmssy-mohfw@gov.in>
To: "Dinesh Kumar"<dinesh.kumar14@nic.in>
Date: Mon, 09 Dec 2024 12:38:31 +0530
Subject: Fwd: CT specifications: 3 different segments
========== Forwarded message ==========

========== Forwarded message ==========
From: <raju152@yahoo.com>
To: "ANKITA MISHRA BUNDELA"<js-pmssy-mohfw@gov.in>
Cc: <shiv223@gmail.com>, <dratinkumar@gmail.com>, <devammc@gmail.com>, <deepakbarathi@gmail.com>, <pushpinderkhera@gmail.com>, <drajaygulati@gmail.com>, <jineesh174@gmail.com>, <anitparihar@gmail.com>, <averma@bhu.ac.in>, <raju152@yahoo.com>
Date: Mon, 02 Dec 2024 23:29:26 +0530
Subject: CT specifications: 3 different segments
========== Forwarded message ==========

Dear Ma'am,
I am attaching the CT specifications in three different segments (**High end 256 slice; Mid end 128 slice and Low end 64 slice**).
The committee has discussed and approved these specifications.

Regards
Raju

Dr Raju Sharma
MD,MAMS,FICR
Professor & Head
Department of Radiodiagnosis & Interventional Radiology
All India Institute of Medical Sciences
New Delhi 110029
Tel (off): 91-26594238
Mob: 91-9810359855

3 Attachment(s) selected • Download as Zip • Add To ›

High End CT.docx.pdf
196.8 KB •

128-Slice Mid End CT.pdf
152.1 KB •

64 Slice CT Low End Specifi... .pdf
97.5 KB •

Sl. No	Technical Specification for 256 Slice CT scanner
	The system quoted should be latest state of art top of the line. The system should have **192 or 96 + 96 or more physical independent rows of detectors capable of Dual Energy applications**. The scanner should be capable of comprehensive whole-body imaging including cardiac, abdomen, neuro and vascular imaging applications, true isotropic volume acquisition. It should also be capable of 3-D reconstructions at fast speeds, quantitative calcium scoring in the vessels using all documented quantification algorithms, 3-D image display during acquisition on-line as well as real time, 3-D vessel imaging with feasibility for volume rendering.
	The AERB compliance for the equipment and its installation would be the responsibility of the supplier.
	The offer should meet the specifications as followed:
1	**Gantry:**
a	The CT Scanner should have low Voltage Slip Rings incorporated in the Gantry
b	The Minimum scan time for a 360 Degree rotation should be less than or equal **to 0.28 seconds or better**
c	The gantry should be provided with User control panels on either side for easy positioning.
d	The sub millimetre Slice @ **0.67 mm or less** in **192 physical rows / 96+ 96** as sandwich arrangement of detector and should be able to acquire **256 slices or more** per rotation. The system should be in position to perform **256 or more** acquisition Slices per Rotation for general, cardiac/vascular applications. Vendor should specify the Z - axis total detector width.
e	The Gantry should have 3D Positioning Laser lights.
f	The Scan field of view (FOV) in acquisition mode should be at least from 250 mm to 500 mm with intermediate Steps for scanning different anatomies.
g	Aperture should be at least **75 cm diameter or more**
2	**X ray Section:**
a	The X ray Generator should be compact and inbuilt in the Gantry.
b	The System X ray power should be 100 kW (actual power) and above.
c	The mA range available should be **between 20 to 1000 mA or more** with increments in steps of not more than 10mA.
d	The X ray Tube should be essentially Dual Focus. The heat storage capacity should be at least **8 MHU or equivalent or more.** Specify the method and technique of cooling
e	Any special feature of the X ray tube to be highlighted with literature.
f	Specify the focal Spots of the X ray tube.
g	The X ray tube should have a cooling rate of not less than 1000 KHU per MIN
h	The X ray tube Cooler Unit should be in built in the Gantry.
3	**Detectors:**
a	The Detector Offered should be Solid State. Specify the Material.
b	**The 256 slice or more acquisition per rotation should be possible**. The System should have **at least 192 rows or 96 + 96** Physical Rows of the detector or more.
c	Specify the Fan Angle of the X rays and the geometry. The detectors should not require frequent calibration.

4	**Patient Couch:**
a	The patient table offered should have a minimum load bearing capacity of at least 150 KG.
b	The Minimum table top height should not be more than 65cms from the floor level for easy transport of trauma patients.
c	**The table top width should be at least 40 cms for better comfort.**
d	The range of metal free scan should be at least 200 cms.
e	The vertical range should be at least 40 cms (max height — min height)
f	Specify the reproducing accuracy of the table.
g	Remote UP/DOWN, FWD/BWD of the Patient Couch should be standard.
5	**Topogram:**
a	Views: should be feasible in frontal and lateral views
b	Should be possible to interrupt acquisition manually if necessary.
6	**Spiral/Helical Section:**
a	The system offered should have Spiral Capability of 60 seconds or above. Real Time Spiral @ 10 f/s should be standard.
b	The range of Spiral facility in Axial Direction should be more than 100 cms.
c	The Reconstruction Time in Spiral scan should not be more than **110** milliseconds.
d	The system should have the Smart Prep or equivalent facility & ability to track Contrast medium to trigger scan should be included in the scope of Supply
e	High Resolution scan package should be offered as standard and specify the minimum slice thickness for which High Resolution scan package is possible.
f	Multi Slice CT Fluoroscopy to be quoted as standard.
7	**Console & Workstation**
a	The Console offered should be the Latest Multi-tasking Processors and a menu driven platform with a RAM size of at least 32 GB.
b	CT console should be of dual monitor design. The Monitor should be: Medical grade, Colour TFT/LCD. The Twin Monitor system should work on either shared or Common data base.
c	The display matrix should be at least 1024 x 1024.
d	The reconstruction time for an Axial scan should not be more than 100 milli seconds.
e	The Hard disk Capacity for both Image and Raw data should be 1 TB or more.
f	It should have facility to store at least 5,00,000 Images
g	The system should be supported with archiving facility of DVD & CD Main Console
h	DICOM facility to send, store, print, receive, Query / Retrieve, MWM, MPPS etc should be standard.
i	Patient radiation dose should be displayed on the monitor as well as on the patient films.
j	PC Based connectivity should be standard for easy transfer of Images & Report. The image transfer from main console to workstation should be automatic and immediate.

k	Workstations & Server: A multimodality client server architecture-based solution with minimum concurrent 40000 slices rendering capacity, with 64 GB RAM or better with total storage of minimum 20 TB **(internal/external)**. Client hardware specification- 2 nos Workstation with dual energy licences for all dual energy applications on each workstation: quad core processor or better, 16 GB RAM or better, 1TB hard drive or better, DVD Writing with medical grade monitor of minimum 2 MP resolution or better & 3 button mouse. The server client solution offered should be OEM. Concurrent licence should be offered for all software/application and should process simultaneously on all the offered workstation at the same time point.
8	**Applications to be offered as standard:**
a	The system should have standard software like 3D Volume rendering, MIP, CT Angio, colour Angio Display, CT Perfusion, should be available as standard on the system
b	The following software should be offered as standard (MPR, Minimum and maximum intensity projection. 3D volume rendering, 3D SSD (Shaded Surface Display). ROI, volume calculation, CT number display, window width, window level, topogram display, cine display, HRCT lung, dynamic scan)
c	Cardiac Scan Attachment with ECG Gated Segmented Recon, Calcium score, Vessel Flythrough of the Coronaries should be available with software package.
d	Automatic display of MPR Images after scan will be preferred.
	Whole organ (brain & body) perfusion CT: Scanner should have capability of Whole brain acquisition of **Minimum 14 cm of coverage**.
e	Bolus triggered Brain Perfusion CT study (at least 3-level) with automatic CBF, CBV, MTT, TTP maps, ROI placing, comparing ROI, saving maps
f	Neuro DSA with automatic bone removal software. Automatic bone removal for other body parts also
h	Fusion CT: fusion of morphological data obtained on CT, MR or DSA.
i	Dynamic CTA with a coverage of **16 cm or more** to cover large areas greater than detector width
j	Dynamic 4D CT should be provided.
k	Metal Artifact Reduction (MAR) should be offered
l	Stroke Analysis & Quantification should be offered
m	Complete Liver Volumetry & Segmentation should be offered
n	CT Virtual endoscopy and Colonoscopy with detail quantification should be offered
o	Advanced vessel analysis.
p	Time point comparison.
q	Coronary tree analysis: automated 3D processing of coronary arteries, calcium scoring, stent analysis, LV analysis.
9	**Dual Energy Applications:** Dual Energy Applications to be provided as standard – Renal Calculi Characterisation, Gout, Lung perfusion & pulmonary emboli detection, Vascular plaque characterisation, Virtual NCCT, Direct Neuro CTA, Contrast vs blood differentiation, Monoenergetic imaging, Endo leak assessment, Virtual non calcium (Bone marrow edema detection), Metal Artifact Correction / Beam Hardening artifact Correction, Brain Haemorrhage Dual Energy Application must be possible on all workstation and all fields of view with minimum FOV **35cm**.
10	**Additional Application** (may be added by local institution as per their requirement – only as optional)– This may be provided on additional cost, the price of which should be separately mentioned Coronary analysis (Optional) **- Minimum** 2 nos of concurrent users should be possible. Cardiac including myocardial perfusion (Optional)

11	**Dose reduction Techniques:**
a	Noise Suppression protocols to maintain LCR at low dose should be standard.
b	Special Softwares (Like MA Modulation in Routine & Cardiac Mode) to ensure Dose efficiency should be standard.
c	Specify the CT Dose Index.
d	Should have model based iterative reconstruction technique (ASiR-V /VEO/ADMIRE/IMR/ AIDR) for X Ray dose reduction. If VEO is not available, vendor should submit an undertaking from OEM. **Also vendor should offer the latest and best available iterative reconstruction available in the offered system during participation of bid.**
e	Low dose Paediatric CT mode should be available
f	Radiation dose reduction technique i.e. mA modulation in X, Y & Z axis, etc.
g	Patient radiation dose should be displayed on the monitor & patient films.
12	**Accessories: (Make and Model of all the quoted accessories should be specified)**
a	Dry chemistry Camera / printer should be of Agfa or Fuji or equivalent with Resolution: 16 bits/ 500 dpi or more with minimum three ports. Support Multiple Film Sizes: one of which must be 17"x14". DICOM 3.0Compatible.
b	Lead Glass as per AERB norms: 200 x 100 cm or better
c	UPS with Maintenance free batteries capable of 30 minutes back up to run the entire CT, Computers, Dry chemistry camera, Work Stations etc. It should be covered under 5 years warranty followed by duration of CAMC.
d	Dual head pressure injector: Dual head pressure injector (of any make) with Synchronization with CT Scanner, with dual flow with 100 nos of Syringes of 200 ml & 300 sets of necessary tubing (with check valves to prevent saline and contrast mixing) and connectors. Unit price for disposable syringe and tubing set should be quoted separately and the same should be valid during warranty period.
e	One Multi parameter monitor of 10 inch or higher for patient vitals (BP, ETCO2, SPO2, Pulse, IBP etc) should be provided, it should have all connecting accessories for adult, paediatric & neonates) also should have IBP interface cable-2nos, and IBP disposable transducer 10nos, IBP Y cable-2 nos *All accessories should be for neonates, paediatric & adult separately)
f	Light weight lead aprons (0.25mm Lead equivalent) with hangers - 4 Nos.
g	Lead apron stand — 1 No.
h	Thyroid Shields – 2 nos.
i	Gonadal Shields – 2 nos.
j	LED X-ray Film viewer with adjustable brightness; capable of holding 3 films of 14"x17" size. – 2 no.s
13	**Additional Optional Accessory (maybe added as per requirement of local institution) –** **1. Anaesthesia Workstation** **Suggested specifications given as Annexure 1. However, the local institution may get it vetted by the anaesthesia department**
14	On Site Training for a period of 4 Weeks.
15	**Certifications:**

I	Should have import/manufacturing license from Central licensing Authority or State licensing authority of CDSCO for Medical Devices and copy of valid license should be submitted for the quoted model. In case the vendor has not yet obtained import/manufacturing license from CDSCO for the quoted model, proof of application for CDSCO medical device license to be submitted in the bid document and valid CDSCO license to be produced at the time of supply/ NOA for the quoted model
II	The system should be AERB type approved and the copy of E-LORA Listing should be submitted along with bid. If the quoted model has not been yet installed in India, vendor should submit NOC from AERB.
III	Regular QA according to AERB norms will be responsibility of bidder during warranty and CMC period.
IV	Offered system should be BIS / European CE with 4 digit notified body no / USFDA certified.
16	**Turnkey (Suggested broad guidelines provided – To be modified as per the requirements and norms of the local institution)**
1	The scope of work includes complete Civil work, Electrical, Plumbing, Furnishing, Airconditioning and Fire detection system for the construction of CT Scan Centre
2	While preparing the plan, the following aspects have to be addressed.
a)	Care should be taken to provide easy negotiation of the patient stretchers/ trolleys through corridors and doors.
b)	Radiation shielding for doors, walls, windows etc.
c)	Furniture like desk, chairs, shelves etc.
d)	Patient stretcher and other furniture/ accessory to make the scan centre functional.
3	The cost of Site Modification for the area of 1000 sq. Ft and Air-conditioning of Tonnage 20 TR (including standby unit/s) will be considered for Ranking / Evaluation purpose. Total capacity of the Air-Conditioning (duct-able) for the entire CT scan centre area should be at least 20 TR (incl. standby air-conditioning) with humidity control between 55-60 % RH
4	Moreover, Bidders will have to quote the Unit Rates of the following components of site modification work.
a)	Civil works
b)	Electrical work
c)	Public health (plumbing and sanitary fittings).
d)	Air Conditioning (HVAC)
e)	Interior Furnishing & Furniture
f)	Miscellaneous
	Fire Detection system (consisting fire panel, smoke &heat detectors, hooters, response indicators etc.) for the entire CT area
	Scope of Site Modification work for CT unit:-
	The scope of work includes complete Civil work, Electrical, Plumbing, Furnishing, Air-conditioning and Fire detection system for the installation of CT centre
	The CT SCAN CENTRE shall consist of the following rooms:
a.	CT Gantry Room
b.	Console room
c.	Equipment room
d.	Patient preparation room cum change room
e	Radiologist room (if space available)
	The actual area of site modification works done will be considered for payment, based on the unit rates and site measurements based on the area available.
	Civil work

a)	Civil construction work including construction of brick wall if any, plastering, flooring as per the approved plan and equipment layout plan.
b)	Concrete bed at CT equipment area.
c)	Platform for unloading and shifting the CT should be provided if necessary.
d)	Cable tray, trench & channel – necessary trenches, cable tray and channels at required location would be provided.
e)	All the construction work to be done as per the final plan approved by the Consignee.
a)	**Flooring**
1	Flooring: - 600 x 600 mm vitrified tiles with 100mm tile skirting to match in Gantry & console room, lobby and patient preparation areas, Radiologist room etc
2	50 mm thick cement concrete flooring with Vinyl flooring in CT equipment / UPS room.
b)	**Painting**
1	Two coats Plastic Emulsion Paint over 2 coats of wall putty including primer in patient preparation area, Lobby area, console room & Equipment room and Radiologist room etc. Full height wall tiles should be provided in the CT Gantry room.
c)	False Ceiling
1	Acoustical tile for ceiling with light weight insulating material of high quality supported on grid or finished seamless with support above ceiling. Finished with white paint or powder coated with white paint, if metallic. Ceiling height to suit the equipment mount and clearances.
	Plumbing work
1	All water pipes and fittings shall be of high density polythene of approved and standard make. The gratings shall be brass chrome plated. All plumbing accessories should be of standard make.
2	Hot water service to be provided if required. (The water supply line and drain line will be provided by consignee upto CT complex)
	Electrical work
1	The supplier shall be required to specify the total load requirements for the CT scan centre including the load of air conditioning , room lighting and for the accessories if any. The supply line will be provided by the Institute up to one point within the CT Scan centre area. The distribution panel shall be provided by the vendor. Few lights in each room shall be connected to the UPS to provide emergency lighting.
2	The electrical work shall include the following:
a.	Wiring – All interior electrical wiring- with main distribution panel board, necessary MCBs, DB, joint box, switch box etc. the wires shall be of copper of different capacity as per the load and should be renowned make as listed below.
b.	Switches light and power points should be of modular type and of standard make as listed below.
c.	General lights – LED light fittings with 500 Lux Illumination
d.	Adequate number of earthing required for equipment and accessories should be provided by the equipment vendor.
3	**AIR CONDITIONING:**
	Ductable Split / Ductable package air conditioners may be used according to room requirement and suitability. Humidity control should be effective to eliminate moisture condensation on equipment surface. The Air conditioning should be designed with standby provision to function 24 hours a day.
	The outdoor units of AC should have grill coverings to prevent theft and damage.
	Ventilation is required in toilet.
	Dehumidifier of 110 Liter - 2 Nos. to be provided

2	**Environment specifications:**	
a)	Relative Humidity range: To be maintained between 60% and 80% in all areas except equipment room which shall be as per requirement of the equipment.	
b)	Temperature ranges: 22± 2° C in all areas except equipment room which shall be as per requirement of the equipment.	
c)	Air conditioning load: The heat load calculations and maintaining the desired temperature and humidity shall be the responsibility of the bidder.	
	Furniture:	
a	Revolving chairs height adjustable, medium-back with hand-rest in the Control room, Radiologist room and viewing area. – 4 NO.S	
b	Cupboard with laminate door shutters for storage of spare parts and accessories and records as per requirement. – 3 NO.S	
c	Drug trolleys 1 numbers for patient preparation area.	
d	Patient trolley with rubber foam mattress to be kept in the patient preparation room.	
e	Name boards for all rooms	
f	Tables for Workstation and Radiologist - 2 NO.S	
g	Changing rooms should have change lockers and dressing table.	
h	Dustbins: 10 no.s	
i	Any other furniture item as per requirement.	
	All furniture items should be of standard make as mentioned in the table below.	
	Miscellaneous:	
1	Cabling of Network (LAN) connectivity for camera system, console system, workstation and computers etc.	
2	Fire extinguisher Dry CO2 type as required for the building safety.	
	LIST OF ITEMS AND SUGGESTED MANUFACTURERS.	
	ITEMS	**PREFERRED MAKES**
A	**FLOORING VITRIFIED TILES**	-Somany, Kajaria , H&R Johnson, RAK india
B	**PAINT**	- Dulux, Asian Paints , Nerolac
C	**PLUMBING**	- Kohler, Jaguar , Grohe , Roca
D	**SANITARY ITEMS**	- CERA, Hindware, Parryware
E	**ELECTRICAL**	
1	**CABLES**	- Finolex, Havells ,V-Guard
2	**SWITCHES**	- Legrand, L&T, Crabtree , Roma
3	**DISTRIBUTION BOX , MCB**	- Legrand, L&T, Siemens, Havels
4	**LIGHT FITTINGS**	- Philips / Crompton / Wipro/syska
F	**AIR CONDINTIONING**	- Daikin, Hitachi, Blue Star, Voltas,
G	**FURNITURE**	- Hermen Miller , Godrej , Featherlite,Geeken
Sl. No	**BILL OF QUANTITY**	
1	**High End Dual Energy CT Scanner** ,as specified	
2	Servers: as specified	
3	Workstation Nodes: as specified	
4	Dry Chemistry camera : as specified	

5	Lead Glass of 200 x 100 cm
6	UPS with Maintenance free batteries
7	Dual Head Pressure Injector
8	Pressure Injector Syringes
9	Tubings for Pressure Injector
10	Multi Para monitor: as specified
11	ULTRA LIGHT WEIGHT lead aprons
12	Lead Apron Hanger
13	Lead apron stand
14	Thyroid Shields
15	Gonadal Shields
	Components of Site Modification Work:
1	Civil works
2	Electrical work
3	Public health (plumbing and sanitary fittings).
4	Air Conditioning
5	Interior Furnishing & Furniture
6	Miscellaneous items
	Furniture:
1	Revolving chairs height adjustable, medium-back with hand-rest.
2	Cupboard with laminate door shutters
3	Drug trolleys for patient preparation area.
4	Patient trolley with rubber foam mattress
5	Tables for Workstation and Radiologist.
6	Changing rooms (with change lockers and dressing table).
7	Dustbins
8	Room Signage
9	Venetian Blinds
	Miscellaneous:
1	Cabling of Network (LAN) connectivity for camera system, console system, workstation and computers etc
2	Fire extinguisher ABC type of 2kg each as required for the building safety
3	Dehumidifier of 110 Liter

Annexure 1

ANESTHESIA WORKSTATION WITH ANESTHESIA MODULAR MONITOR : Qty 1

Anesthesia workstation is used for delivering anesthesia agent to the patient during CT

A. It should be integrated anesthesia workstation
A. It should offer ICU quality ventilator, suitable for adult, children & neonates.
B. Single user interface should control and display all parameter including control of modes, display of cylinder pressures etc.
A. The machine should be suitable for low and minimal flow anesthesia application
A. The machine should have automatic calculations and presetting of patient specific ventilation settings
B. It should have configurable screen layouts for individual screen set ups.
C. It should have Nitrous oxide free operation configurable
A. The anesthesia machine and vaporizer should be manufactured by same company.

1. The Anesthesia Machine capable of providing anesthesia to Adult, Paediatric and Neonatal patient should have the following:
    a. Should have pipelines attachment for oxygen, nitrous oxide and compressed air.
    a. Should have yoke assembly for oxygen and nitrous oxide with pin index system.
    b. Durable main switch to put the machine in the on or off position.
    c. There should be digital control and display for oxygen
    d. There should be electronic gas mixing.
2. Should have safety features like :
    a. Should be provided with" pneumatic/electronic" hypoxic guard.
    a. Should provide 25% or more of oxygen when an anesthetic gaseous mixture is in used.
    b. Should have extra flow meters for oxygen only.
    c. Should have digital display of pressure value of Cylinders and Central pipeline
    0. Should have oxygen flush with a flow rate of more than 35L/min.
    0. **Vaporizer – New generation**
    a. Should be able to hold two vaporizers (Isoflurane, Sevoflurane & Desflurane) simultaneously.
    a. Cost of vaporizers to be quoted separately.
    b. Quantity of vaporizer to be purchased will be as per requirement.
    c. Temperature / pressure compensated and flow independent vaporizer.
    d. The vaporizer design should be maintenance free.
    e. Should have illumination of vaporizer setting and filling level
    f. Should preferably have electronic monitoring of vaporizer setting and filling level
    0. **CO2 absorber system** with the following features :-
        a. Single/Double canister
        b. Autoclavable
        c. Canister capacity of 0.8 kg or more.
        d. It should be possible to bypass the canister if removed during clinical cases to change soda lime.
    0. APL valve assembly and Bag mount should be conveniently placed.
    0. Independent port for open circuit.
    0. Should be provided with drawers for storage space
    0. Machine should have a good quality handle and castors to move the machine with locking system.

0. The ventilator of the machine should have the following features:-
   a. Should be electronically controlled.
   b. Should be suitable for new born, pediatric and adult
   c. It should have colored screen with minimum 12" screen size.
   d. Volume and pressure control mode of ventilations.
   e. Electronic PEEP
   f. Various ventilator modes: SIMV, pressure support, VCV, PCV modes etc
   g. Tidal volume range from 20 ml to 1200 ml
   h. Respiratory rate from 4 to 80 or more
   i. I:E ratio 2:1 – 1:5
   j. Display: Respiratory rate, peak airway pressure and PEEP
   k. There should be no collection of water in the breathing system
0. Should have independent **paramagnetic** oxygen sensor for FiO_2 monitor and flow sensor for spirometry loops.
0. Should be able to display
   a. Pressure Vs time
   b. Volume/ Flow Vs time
0. The work station should be capable of delivery of low and minimal flow anesthesia even at 350 ml of total fresh gas to reduce patient consumption
0. It should have alternate O2 supply mode in case electronic gas mixture failure.
0. Should have a battery backup of at least 60 minutes
0. A demonstration of the product is essential by the firm of the model quoted
0. **Monitor** should have the following
a. A modular configurable patient monitor for adult, pediatric and neonatal patient
a. Should have at least 19" or more TFT color display with a minimum of 8 waveforms at a time.
b. Should be touch screen
0. **Should be able to measure the following parameters:**
   a. 3 and 5 lead ECG with electrocautery & defibrillator filter with ST Segment & arrhythmia detection with analysis,
   b. Respiration , SpO2 (SpO2 technology to prevent motion artifact), temperature
   c.SpO2 with Masimo technology to prevent motion artifact
   d. NIBP, IBP , ETCO2
   e. Multi –Gas analysis with auto detection of all anesthetic agents
   f. Integrated BIS/entropy Monitoring.
0. Should be able to automatically detect and calculate MAC of all anesthetic gases. There should be no electrical RF interference.
0. Should be able to calculate and display FiO2.
0. Intelligent cooling system to keeps the unit running quiet during use.
0. Separate indicator lights for technical and physiological alarms.
0. Maximum BEEP tone should be loud enough to be audible from at least a distance of 12 feet.
0. Should have graded audio and visual alarms for the following parameters:
   a. Blood pressure - High and Low
   b. SpO2 - High and Low
   c. Heart rate - High and Low
   d. Respiration - High and Low
   e. FiO2 - High and Low
0. Trends – Upto **48** Hours or more
0. Display of Anesthesia ventilator data like wave forms for flow, pressure, agent and loops, and trends on patient monitors.

0. It should be ready to run Web based application like PACS, HIS, RIS, LIS, Cath lab Report, X-Ray as standard on the patient monitor
0. All the components like anesthesia ventilator, vaporizer, and patient monitor should be preferably from same manufacturer.
0. The quoted model should be European CE or US FDA approved
0. The machine should be supplied with the following accessories:
   a. ECG Cable – 10 Nos
   b. Reusable SpO2 Sensors: 5 each for Adult, Pediatric & Neonatal.
   c. NIBP Cuff: 10 each for Adult, 5 each for Pediatric & 5 Neonate.
   e. IBP Cable: 10 nos
   f. BIS / Entropy Electrode – 50 to be given against staggered demand
   g. ETCO2 Sample Line: 50 nos with each machine
   h. Water trap 50 nos. with each machine
   i. Reusable autoclavable Breathing circuit: 25 nos each for Adult & 5 pediatric
   j. Temperature Probe – 1Paed , 4 Adult (skin)
   k. Isoflurane, Sevoflurane & Desflurane Vaporizers. Cost of vaporizers to be quoted separately.
0. Disposable breathing circuit including water trap- 50 each for adult and pediatric. Reusable anesthesia mask 10 set for adult, 5 pediatric and 5 neonate.
0. System should have facility and required accessories for suction and active AGSS (Anesthesia gas Scavenging System)(From same OEM)
0. Please provide Accessories which would last for one year.
0. Demonstration is must.
0. **System should have Web based Anesthesia Charting facility. Prices to be quoted separately along with Server and complete wiring.**
0. **Scope of Supply :**

a. Trolley with drawer
a. Writing surface
b. Pin Index yokes for O2 & N2O
c. Pipeline connections for all three gases
d. Integrated Ventilator & monitor
e. Semi closed breathing system
f. Adult & pediatric autoclavable patient tubings- as asked above
g. Anesthetic mask (silicon) size – Adult & child- As asked above
h. Vaporizers for Isoflourane, Sevoflourane, Desflurane- (f As asked above one machine ly)
i. Central gas supply hoses (Color coded)
j. Instruction for use

0. Should be European CE marked/FDA marked
0. Vendors should also quote the price for SPO2 probe and BP Cuff, IBP transducers (Pediatric & Adult), ECG leads separately for the further purchase if required and the same should be valid during warranty and CMC period.

All the probes and accessories both for Adult & Pediatrics age groups should be provided for 10 years.

A demonstration of the product is essential by the firm of the quoted model and must provide preferably a performance certificate of the model quoted.

Technical Specifications for CT scan with 32 physical detector rows.

Description
Whole Body CT Scanner with sub mm acquisition for entire 32 physical detector rows and 64 slice reconstruction or better.
Gantry
1. The CT scanner should have low Voltage Slip Rings incorporated in the Gantry.
2. The Minimum scan time for a 360 Degree rotation should be 0.8 Second or less.
3. The gantry with mechanical/digital tilt of upto ±24 ° or better.
4.The gantry should be provided with a user control panel or Mobile tablet and remote control for easy patient positioning.
5. CT Should be capable of acquiring sub mm slices 32 slices for entire 32 physical detector rows with slice profile of 0.7 mm or better. System should be able to generate/reconstruct 64 slices or better per rotation.
6. The Gantry should have 3D Positioning Laser lights, with a patient observation camera if possible.
7. The Scan field of view (FOV) in acquisition mode should be 5–50cm with intermediate steps for scanning different anatomies. System should have an extended FOV of 700 mm or better.
8. Aperture should be of 70 cm in diameter or more.
X ray Tube:
1. The X ray Tube current should be 13 to 350 mA or more with increments in steps of not more than 10 mA.
2. The system should work combined with the latest iterative reconstruction technique to avoid excess radiation.
3. Generator should be compact and inbuilt in the Gantry.
4. The System X ray power should be 32 KW or above.
5. Tube Voltage should be variable from 80 to 130 kV or better.
6. The X ray Tube should be with a capacity of at least 3.5 MHU. Any special feature of the X ray tube to be highlighted with literature.
7. Tube should have dual focal spots to adapt to various imaging needs.
8. The X ray tube should have a cooling rate of 900 KHU/min or better
9. The X ray tube Cooler Unit should be built in the Gantry.
10. The System should be Equipped with Ultra Low Dose Technology, Specify the Technology with detailed Technical Data On it.
Detectors:
1. 32 slice acquisition per rotation should be possible with the detectors in sub-mm mode. Detector should have a minimum physical 32 rows of detector with capability to reconstruct 64 slices or better.
2. In-built mechanism for adapting the tube current during each scan. This should enable radiation dose reduction where body part thickness is less. Specify mechanism used in the system.
3. The detectors should not require frequent calibration.

Patient Table:
1. The patient table offered should have a minimum load bearing capacity of at least 200 kg
2. The Floating tabletop width should be at least 45 cm or better for better comfort. The vertical range of travel should be at least 40 cm or better patient comfort.
3. Specify the reproducing accuracy of the table.
4. Remote UP/DOWN, FWD/BWD of the Patient Couch should be standard
Spiral / Helical Section:
1. The system offered should have Spiral Capability of at least 120 seconds or better.
2. The range of Spiral facility in Axial Direction should be 150 cm or better.
3. The Image reconstruction Time should be at least 20 Images / second or better.
4. Bolus triggered spiral acquisition should be possible
5. High Resolution sub mm slice thickness with 32 row acquisition should be offered as standard.
6. Slice thickness should be 0.625 mm to 10 mm or better.
Main Console Computer Section:
1. The main console CPU offered should be the Latest Multitasking Processors and a menu driven platform with a RAM size of at least 32 GB DDR2
2. The Monitor should be the Latest Coloured of at least 24 inches or better and flat screen. There should be a Console with One large 24 inch monitor or better.
3. The display matrix should be at least 1024 x 1024.
4. The Hard disk Capacity for both Image and Raw data should be more than 700 GB or better.
5. It should have a facility to store at least 600,000 Images or better.
6. The Main Console should have standard software like 3D Volume rendering, MIP, CT Angio, Colour Angio Display, 3D Artifact Suppressions, Pre-set 3D Reconstruction & Display Protocols, Auto Bone Removal, Endoscopy and Vascular assessment. Direct generation of axial, sagittal, coronal, or double-oblique images from standard scanning protocols.
7. The following software should be offered as standard (MPR, ROI, Volume Calculation, CT Number Measurement of between –8, 000 to + 35000 or better, Window Width, Window Level, Topogram Display, Cine Display etc.
8. The system should be supported with the archiving facility of DVD & CD in the Main Console.
9. DICOM facility to send, store, print, receive, Query / Retrieve, MWM, MPPS etc should be standard.
10. Calcium Scoring Software should be provided for visualization and quantification of calcified coronary lesions volume, calcium mass and total Agatston equivalent score.
11. Dedicated Metal artifact correction software should be offered.
Resolution:
1. Specify the System Spatial Resolution.
2. The low contrast resolution should be 3 mm at 3HU difference or better.
3. Noise Suppression protocols to maintain LCR at low dose should be standard.
4. Special Software's (Like MA Modulation in Routine) to ensure Dose efficiency should be standard.
5. Specify the CT Dose Index

ADDITIONAL ACCESSORY TO BE QUOTED AS OPTIONAL
(This may be added by the local hospital as per their requirement). The price for the same to be quoted separately

OEM Post Processing Workstation for CT:

a. Standalone multi-modality independent workstation with same user interface as the console computer from the same manufacturer as the CT Scanner
b. Minimum Hardware : 3.0 GHz 6 Core CPU, 32 GB RAM, 1TB SSD, 4GB GPU, standard Keyboard & mouse, 1.5 kVA UPS, 24" 2.3 MP Medical Colour Monitor.
c. Should be capable of performing CT post processing functions and filming independent of the main console. Two-way data transfer between the operative console and the postprocessing workstation should be possible.
d. Statistical evaluation tools: Area / volume, Standard deviation, Mean value, Min. / max. values
e. Image evaluation tools: All advanced post processing softwares like MIP, MPR, CPR, VRT, Image Fusion, Neuro Subtraction, CT angiography for both brain, body & extremities, Table & Bone Removal tools, Virtual Endoscopy, Vessel analysis, Vessel segmentation

Accessories:
1. Dry / Laser Imager of any reputed make.
2. Lead Glass of at least 2 ft by 4 ft
3. UPS with 30 minutes back up of suitable capacity to handle CT Computer, Imager, Workstation
4. Single Head Contrast Injector of reputed make with compatible 100 syringes and 500 tubings.
Turn key : (to be given by the local hospital as per the space and local requirements)

128-Slice CT Scanner Standard Technical Specification

Technical Specification		
State of the art Whole body 128 Slice CT Scanner having capability to perform both axial and spiral mode system for data generation/acquisition. The quoted model should have latest iterative reconstruction technology for dose reduction. Quoted model should have all latest applications & upgrades as available with the vendors at the time of applying. The quoted model must be Latest Generation & Version released by the vendor. Further undertaking for 10 years' service and spare parts availability to be submitted on authorized letterhead.		
S. No.	**GANTRY**	
1.1	Aperture	≥ 70 cm
1,2	Scan field	≥50 cm
1.3	Integrated Display Panel	Gantry front showing patient and/or machine information.
1.4	Laser Lights	The gantry should have 3D positioning Laser lights
1.5	Gantry Physical/Digital Tilt	± 24 degree or better
2	**X-RAY GENERATOR**	
2.1	Output capacity (actual and not effective)	≥72 kW
2.2	Continuous Helical / Spiral Time	≥100s
3	**TUBE ASSEMBLY**	
e.1	Tube Voltage	80-135 kV or better
3.2	Tube current range	20-600 mA
3.3	Dual Focal spot size	(as per IEC 60336: 2005)
3.4	Tube Heat loading capacity	≥7.0 MHU or higher
3.5	Scan time for full 360-degree rotation	<= 0.35 sec
3,6	Tube cooling	≥1000 KHU/minute or better
4	**DETECTOR**	
4.1	Number of slices	Ability to acquire / generate 128-slices / 360-degree rotation
4.2	Pitch	Pitch should be Freely selectable between 0.5-1.5 or more
4.3	Range of slice thickness (Axial Mode)	0.625 — 5mm or better
4.4	Number or physical rows	64 physical rows or more
4.5	Detector width	38 mm or more
5	**PATIENT TABLE**	
5.1	Maximum load capacity	≥ 200 kg,

5.2	Scannable range	≥ 1500 mm
5.3	Longitudinal table speed	≥ 150mm per sec
5.4	Table Positioning	Reproducibility of table positioning (mm) should be +/ - 0.25 mm or better
5.5	Table dimensions	Specify the width and length of the table, distance between gantry front and table base (minimum and maximum should be specified)
6	**SCANNING PARAMETERS**	
6.1	Cardiac imaging	The quoted system should be able to generate image with single or multi sector reconstruction for patients with heart rates ranging between 60-100/min. and with temporal resolution of 175ms or better for single sector recon and 44ms or better with multi sector reconstruction will be preferred.
6.2	Iterative reconstruction based single exposure metal artifact reduction	(iMAR / SmartMAR / O-MAR / SEMAR) or equivalent should be offered as standard
6.3	4 D dynamic scanning	like – Jog Mode/Volume Helical Shuttle/Flex 4D Spiral or equivalent scan techniques with minimum 8cm coverage or more
7	**APPLICATIONS TO BE INCLUDED IN STANDARD PACKAGE**	
7.1	Metal Artifact Reduction (MAR) software	Metal Artifact Reduction (MAR) software
8	**PATIENT COMUNICATION**	
8.1	Integrated patient intercom	There should be Integrated patient two-way communication system capable of playing recorded audio
8.2	Automatic Patient instruction	A standard set of commands for patient communication before, during, and after scanning should be available in English and Hindi language
9	**PATIENT REGISTRATION**	
9.1	Pre-registration	It should be possible to do pre-registration of patient at any time prior to scans
9.2	Emergency registration	Special emergency registration should be possible
9.3	HIS & RIS integration	It must transfer patient information from departmental RIS & HIS via DICOM Work list
10	**OPERATOR CONSOLE WITH TABLE**	
10.1	Operator console should be supplied with chair & monitor adjusting bracket/stand.	
10.2	Storage	Minimum of 4,00,000 images with matrix size of 512x512 should be able to store on console
10.3	Display	19" or more high resolution Medical grade LED/LCD/TFT monitors with a display on 1024X 1024 or better

10.4	DICOM DVD/CD/USB	Should be able to export DICOM format with DVD/CD/USB other than png, jpg, avi, movie etc.
11	**IMAGE POST PROCESSING**	
11.1	**Standalone workstation (quantity – 1)** **Additional 1 workstation may be taken as OPTIONAL depending upon the requirement of the local institution** The price of 1 unit to be quoted separately	**RAM:** 64 GB or Better **Monitor:** Clinical Grade Monitor With 2MP (1024 X1024) or Higher. **OS:** Windows 10/Linux, 64 bit **SSD:** 1TB or Better CD/DVD/USB drive All basic and advanced software asked in the specifications should be available on all workstation(s) The software should also include reputed antivirus software of a perpetual type or renewed by the supplier Filming also should be possible from this client / node / workstation.
12	**Basic & advanced capabilities with exact same license on each**	
12.1	MPR	Real-time multi-planar reconstruction
12.2	ROI Evaluation	Parallel evaluation of multiple ROI In circle, irregular and polygonal forms
12.3	Statistical Evaluation	Area/ volume, Standard deviation, Mean value, Image annotation and labeling, Angle measurement, Distance measurement Histogram, rime intensity curves, Peak enhancement images, Time-to-peak images.
12.4	2-D	2D, including image zoom and pan, image manipulations. reversal of grey-scale values, and mirroring; and advanced bone correction
12.5	3-D	MIP, Min IP, VRT and other advanced 3D applications and color-coding for different tissues.
12.6	CT Angiography	Automatic table and bone subtraction in a angiography, Single click bone removal, manual and automatic vessel tracking, Carotid Stenosis measurement, Single energy calcium removal should be available either on main console or on work station
12.7	CT Perfusion	Software for advanced cerebral perfusion study with stroke protocol and summary maps of the perfused area brain with minimum 8cm coverage to cover whole Brain perfusion.
13	**IMAGE RECONSTRUCTION**	
13.1	Recon speed	Minimum 23 images/sec for
13.2	Recon Matrix	512 X 512& 1024 X 1024
14	**IMAGE QUALITY**	

14.1	High contrast Spatial Resolution for entire width of detector	It should be not less than 15 lines pair per cm or better maximum at 0% or 2% MTF X-Y axis for beam collimation not less than 20 cm on Catphan Phantom
14.2	Low-contrast resolution	The low contrast resolution for CATPHAN should be at least 5mm at 3 HU with 10mm slice on 20cm Catphan phantom. Please mention the dose at which the resolution is achieved,
15	**DOSE REDUCTION TECHNIQUES**	
15.1	Pre-patient collimation	There should be pre-patient collimation to reduce unnecessary dose to the patient
15.2	Advanced Iterative Reconstruction	Latest Iterative reconstruction should be offered with all imaging protocols.
15.3	Cardiac Scanning	Step and shoot technique during cardiac scanning for dose reduction, or a similar alternative technology should be available with arrhythmia correction
15.4	Organ Dose Modulation	Advanced dose limiting for critical organs using ODM/x-CARE or equivalent should be offered as standard
15.5	3D Dose Modulation	Tube current modulation along Z-axis for different patient size and organs should be offered as standard
15.6	Pediatric & Infant Imaging protocols	Low dose protocols must be provided
16	**NETWORKING**	
16.1	DICOM	Dicom Storage (Send/Receive)
16.2	DICOM	DICOM Modality Worklist User
16.3	DICOM	Modality Performed Procedure Step (MPPS)
16.4	DICOM	DICOM Print User
16.5	DICOM	Query/retrieve user and provider
16.6	Integration with department RIS and HIS	Integration with departmental RIS and HIS must be done. Any licenses or software needed for the same is to be provided by the vendor
16.7	Transfer to network nodes	Automatic transfer to all network nodes.
17	**DICOM USB/CD/DVD Writer**	DICOM images USB/CD/DVD Writer
18	**ACCESSORIES**	
18.1	Dual head pressure injector	Dual head pressure injector (of any make) with Synchronization with CT Scanner, with dual flow with 100 nos of Syringes of 200 ml & 300 sets of necessary tubing (with check valves to prevent saline and contrast mixing) and connectors. Unit price for disposable syringe and tubing set should be quoted separately and the same should be valid during warranty period.

18.2	Dry Laser Camera/Printer	Camera / printer should be of Agfa or Fuji or equivalent with Resolution: 16 bits/ 500 dpi or more with minimum three ports. Support Multiple Film Sizes: one of which must be 17"x14". DICOM 3.0Compatible. To be supplied with 500 films of 17"x14"
18.3	UPS Power	Full Load UPS including CT, Workstation Server, Client & Pressure Injector for 30 Min backup with maintenance free batteries. It should be covered under 5 years warranty followed by duration of CAMC.
18.4	Standard Patient positioning accessory and restraining device	All standard Accessories pertaining to patient comfort and desired study like head holder, coronal head rest, arm rest, cushions, and pads, IV pole.
18.5	Lead Glass	Lead glass of size 200 x 100 cm or better should be installed between examination room and console room as on site.
18.6	Multi Parameter monitor	One Multi parameter monitor of 10 inch or higher for patient vitals (BP, ETCO2, SPO2, Pulse, IBP etc) should be provided, it should have all connecting accessories for adult pediatric & neonates) also should have IBP interface cable-2nos, and IBP disposable transducer 10nos, IBP Y cable-2 nos *All accessories should be for neonates, pediatric & adult separately)
19	**ONSITE TRAINING**	In house training should be provided for technical staff and radiologists from an application expert from the principal manufacturer for a minimum period of 4 weeks.
20	**ADDITIONAL ACCESSORIES (may be added or modified or be made mandatory by local institution as per their requirement)– These may be provided on additional cost, the price of which should be separately mentioned**	
20.1	Compatible syringes with necessary tubings (with check valves to prevent mixing of saline and contrast) and connectors for the Dual head pressure injector	1000 (unit price of each to be quoted separately
20.2	Furniture	Five revolving chair and five non-revolving chairs of good quality and make such as Godrej etc should be provided.
20.3	Furniture	Adequate wooden storage in CT console room and gantry room should be provided. Vendor shall do this as per requirement of user department.

20.4	Radiation protection devices	Light Weight lead aprons (0.25mm Lead equivalent) with hangers - 4 Nos. Lead apron stand — 1 No. Thyroid Shields – 2 nos. Gonadal Shields – 2 nos.
20.5	Crash Cart	One good quality crash cart . 4 medium size dustbin for medical waste as per color (yellow (1) ,red(1) , blue(2)), Also one stainless steel IV stand , one steel trolley (dressing trolley) big size.
20.6	Mic system for patient	Mic system for calling patient should be provided with speaker in patient sitting area.
21	**CERTIFICATION**	System offered should have AERB type approval, CDSCO Certification Or FDA Certification Or CE Certification at the time of submission of the bid.
22	**OTHER REQUIREMENTS**	
22.1	Software for Remote Diagnostics Service and reputed antivirus solution of perpetual type or renewed by the supplier over the internet line at no extra cost to the user. Internet connection to be provided and maintained by the vendor.	
22.2	CT machine must be seamlessly connected with existing PACS, HIS/RIS of the local institution, with all necessary hardware or software required for this purpose should be provided by vendor at no additional cost.	
22.3	One good quality crash cart . 4 medium size dustbin for medical waste as per color (yellow (1) ,red(1) , blue(2)), Also one stainless steel IV stand , one steel trolley (dressing trolley) big size.	
23	**ADDITIONAL APPLICATIONS (may be added or modified or be made mandatory by local institution as per their requirement)– These may be provided on additional cost, the price of which should be separately mentioned**	
23.1	ECG Gating	Prospective & Retrospective ECG trigger facility. It should be provided with all the accessories required for adult and pediatric cases.
23.2	Stroke Analysis & Quantification	Stroke Analysis & Quantification software made by OEM
Turnkey (Suggested broad guidelines provided – To be modified as per the requirements and norms of the local institution)		
All work related to turnkey , civil, electrical and AC should be vetted by and should be executed in consultation with user department. The machines are to be installed on the turnkey basis. The details of TURNKEY are provided below.		
Turnkey rooms scope: CT Gantry room, Common Console room, Common Electrical room, Common patient waiting area cum preparation room and store room.		

File No. Z-28016/35/2024-PMSSY-IV-Part(3) (Computer No. 8310053)
Generated from eOffice by SARITA, EA(S)-PMSSY, DEO, DOHFW DEPARTMENT on 28/01/2025 09:57 am

All machine installations and plans to be AERB compliant.
Vendor should provide the wooden customized Storage cabinets in CT gantry room as well as in console room as per the requirement of user department.
5 height adjustable revolving chairs and 5 non-revolving chairs (godrej etc) and 1 stools- each of reputed brand and one foot step of stainless steel.
Addressable Fire detection and fire-fighting system be provided and integrated with hospital system.
Robust Pest/ Rodent control solution for lifetime be provided to protect the installed equipment/ accessories/ electrical cables etc. at no extra cost.
Vendor shall connect the entire CT machine with existing RIS and PACS, printers of the local department for this all required network wiring, ports , switches for entire equipment , workstation, should be provided.
Vendor shall provide the oxygen and suction panel and connect it with existing line of the hospital. All accessories related to this should be provided.
Air Conditioning:
The requirement (tonnage) of air conditioning system must be clearly stated. Air conditioning must be provided for the CT Gantry room, Electrical room, Console room and patient waiting/ preparation room. The temperature of the AC rooms must be maintained at 180C and patient waiting cum preparation area at 200C. Humidity to be kept at 50-60% hours at all times. The AC should be of ductable split type and prevent possibility of water leak; The system must have in built redundancy and back up to cover for breakdown. Temperature display monitor should be installed in gantry room.
Civil Work:
Areas should have complete wall to wall vitrified non-slippery tile flooring, Kajaria or Johnson & Johnson make. Wooden doors with proper lead protection as per AERB recommendations. For flooring of CT Gantry room good quality granite marble stone flooring should be provided.
Civil construction work including construction/modification/demolition of brick wall if any, plastering, finishing work, putty work, acrylic emulsion on walls/ceiling should be done as per site requirement and matching decor. All brick walls should have tiles installed up to false ceiling.
False ceiling – Armstrong metallic false ceiling and gypsum board 12 mm false ceiling wherever required as per site requirement.
Complete water proofing work of the roof of entire CT area with installation of sturdy floor tiles should be provided. Vendor should inspect and discuss with the user department.
Electrical Work:
Specify the total load requirement i.e. required for the machines, air-conditioning, room lighting and accessories. Load will be provided by the Institute up to the main distribution panel. The panel is to be installed by the firm as per requirement of the unit. The firm shall provide electrical supply cables and required switch gears upto the main distribution panel.
Light fixtures should be provided with fluorescent lamp with mirror optic reflectors. Additional/ backup illumination to be provided in the gantry room, electric room console, patient waiting cum preparation area, seminar room and department offices, to cover for outages in emergencies.

Adequate number of wall sockets/ switches to be provided in the rooms. All such sockets / switches should be high quality.
Provision of proper earthing as per power load shall be the responsibility of the vendor.
Fire Safety: Facility should be equipped with firefighting/ extinguisher system and addressable fire alarm be linked to the existing central fire alarm system of the concerned room in consultation with Fire Safety Officer. Fire safety signage be installed in consultation with the fire officer.
Warranty:
Sixty months from the date of satisfactory installation. The warranty shall cover complete CT machine including their X Ray tubes, all accessories, turnkey including, Air Conditioning, Electricals, Civil, furniture, fixtures, computers, servers/ workstation, displays and all other information technology (IT) items supplied and installed with the machines etc. During the warranty period, the protection of equipment and cables from pests/ rodents will be the responsibility of vendor. The cost of the periodic QA tests/ checks as per the AERB norms to remain vendor's responsibility during the warranty and CAMC, at no additional cost to the user.
Comprehensive Maintenance Contract (CMC) for next 5 years, with terms, conditions and coverage be same as warranty, and must be quoted.
Certification System offered should have AERB type approval, CDSCO Certification Or FDA Certification Or CE Certification at the time of submission of the bid.
Instructions To The Vendors/Suppliers:
All bidding companies must visit the site to ascertain the available space/ scope of work before quoting models of their machines & confirm the specifications. No additional space will be provided. Installations must comply with the AERB norms. The vendor to assist the user department in obtaining the AERB approvals.
The compliance statement must be filled strictly under the headings given in the tender. Each specification corroborated in the compliance statement must give the page number where it is listed in the product data sheet. Incompletely filled information will not be considered.

Z-28016/35/2024-PMSSY-IV (8285627)
Government of India
Ministry of Health & Family Welfare
(PMSSY-IV Section)

Room No. 745-A, Nirman Bhawan, New Delhi
Dated the 21-08-2024

Office Order

Subject : Circulation of approved Technical Specifications of 10 Medical Equipment- reg.

In continuation of the office order dated 02-08-2024, please find enclosed herewith the Technical Specifications of following 10 High End Medical Equipment as submitted by the Committee set up by MoHFW under the Chairpersonship of Dr. Raju Sharma, Professor & Head, Department of Radiodiagnosis & Interventional Radiology, AIIMS New Delhi.

2. The above specifications have the approval of Secretary (HFW) and shall be valid for two years. All AIIMS/ INIs/ Institutes/ Hospitals/ Procurement Support Agency (HITES) of the Ministry are advised to adhere to the approved specifications (enclosed) while undertaking procurement of these equipment:

i. Specifications for Flat Panel based Digital Under couch Fluoroscopy Systemwith Ceiling Mounted Radiography unit on turn key basis
ii. Digital Radiography system (1000 MA) with Wireless Dual Flat PanelDetector (mid end)
iii. Specifications of High-frequency over the couch Digital R/F System
iv. Specifications for Digital Mobile Digital Radiography unit (mid end)
v. Technical specification of Mobile DR (low end)
vi. Technical specifications for AI enabled Digital Flat Panel Dual Detector 1000MA X-ray unit (high end)
vii. Technical specifications for Digital Flat Panel Dual Detector 630 MA X-ray unit(low end)
viii. Specifications for High end Digital Mobile Digital Radiography unit (high end)
ix. Specification for Mobile Flat Panel Detector C-Arm unit (high end)
x. Specification for Low end Mobile Flat Panel Detector C-Arm unit (low end)

(Arun Kumar Biswas)
Under Secretary to the Govt. of India
Tel:011-23061730
ak.biswas57@nic.in

Encl (2):

i. Technical Specifications of 10 Medical Equipment

ii. Office Order No. Z-28016/35/2024-PMSSY- PMSSY-IV,dated 02-08-2024To

i. All Additional Secretaries/ Joint Secretaries, MoHFW – with a request to circulate the above specifications to all the Institutes/ Hospitals/ INIs/ Autonomous Bodies under their administrative control, for compliance.

ii. Director General of Health Services, MoHFW, GoI

Copy to :

i. Director, AIIMS New Delhi

ii. Director, PGIMER, Chandigarh,

iii. Director, JIPMER, Puducherry

iv. Director, NIMHNAS, Bengaluru

v. The Directors/ Executive Directors of new AIIMS under PMSSY

vi. The Directors of Central Government Hospitals in Delhi/ North East Hospitals

vii. CEO, HITES (via email at ceo@hllhites.com)

Copy for information to :

i. PSO to Secretary(HFW)

ii. PPS to Joint Secretary (PMSSY)

Gmail

pmssysection iv <pmssysectioniv@gmail.com>

Circulation of approved Technical Specifications of 10 Medical Equipment- reg.

1 message

pmssysection iv <pmssysectioniv@gmail.com> Wed, Aug 21, 2024 at 5:52 PM
To: Asfa-mhfw@nic.in, j_mishra@gov.in, asfr-mohfw@gov.in, Roli Singh <roli.singh@ias.nic.in>, ash-mohfw@nic.in, Zhimomiv@ias.nic.in, Dgoffice@naco.gov.in, Ischangsan@nic.in, asmd-mohfw@nic.in, jstraining-mohfw@gov.in, Pushpendra.r@nic.in, Vandana.jain@nic.in, Robert.elangbam@gov.in, Sinha.vijay@nic.in, Ea-mohfw@nic.in, kk.tripathy@nic.in, r.wadhawan15@nic.in, jsrch-mohfw@gov.in, cca-mohfw@nic.in, anoopk.puri@nic.in, Ddgtb@rntcp.org, pradeep.khasnobis@gov.in, js-pmssy-mohfw@gov.in, js-publichealth@gov.in, Ankita.edu@nic.in, dghs@nic.in
Cc: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, edaiimsrbl@gmail.com, rajwanshiarvind@hotmail.com, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, "Prof. Dr. D.K. Singh, Director" <director@aiimsbathinda.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, shakti810505@gmail.com, cdskatoch@gmail.com, Executive Director AIIMS Rajkot <ed.aiimsrajkot@gmail.com>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, madhabananda@gmail.com, sachimohanty@rediffmail.in, Dr Vivek Lal <dpgi@pgimer.edu.in>, director@jipmer.ac.in, director@aiims.gov.in, Director Neigrihms <director-neigrihms@gov.in>, nalinaiims.mehta@gmail.com, eigasunil@gmail.com, director@ripans.ac.in, MS OFFICE SJH <msoffice@vmmc-sjh.nic.in>, "Dr. Sunita Sharma" <director-lhmc@gov.in>, minakshi Bhardwaj <med.sup@rmlh.nic.in>, ceo@hllhites.com, secyhfw@nic.in, Praveen.batra@gov.in, "Cc:" <Dinesh.kumar14@nic.in>, ":" <ak.biswas57@nic.in>, sankar.garg@gov.in, Amit Batra <amit.batra@gov.in>

Sir/ Madam

Please find the attachment.

Note: In case this email requires you to reply, you are requested to reply to all the officials of PMSSY-IV Section at - dinesh.kumar14@nic.in; ak.biswas57@nic.in; sankar.garg@gov.in; amit.batra@gov.in
Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

3 attachments

Circulation.pdf
554K

Encl 2..pdf
5302K

Encl 1..pdf
12471K

Specifications for Flat Panel based Digital Under couch Fluoroscopy System with ceiling mounted radiography unit on turn key basis	
High powered X-Ray unit with digital flat panel for various fluoroscopy examinations and radiography using ceiling mounted radiography unit	
The unit should be a completely integrated system (integrated X ray generator and image acquisition control console) having the following specifications.	
Generator	
1.	1000mA unit with microprocessor controlled high frequency X-ray generator with power output of 80 kW or more.
2.	Exposure kV range should be 40-150.
3.	System should have a facility for pulsed fluoroscopy.
4.	Generator should have a minimum exposure time of at least 1ms.
5.	System should have multiple user defined programmes (vendor defined programmes).
6.	There should be provision for automatic exposure control (AEC). It should be possible to override AEC if required.
TABLE	
1.	Floor mounted table with radiolucent composite material or carbon fiber table top, scratch resistant surface.
2.	System should have motor driven longitudinal, and horizontal table top movements.Please specify the range of movements.
3.	Table should have angulations from longitudinal to head down positions. (Vertical +90 degrees to Trendelenburg -20 degrees)
4.	Table should support a patient weight 185 kgs or more.
5.	System should have a well designed foot switch for releasing fluoroscopy and acquisition.
6.	System should have provision for collision protection.
7.	Table should have an integrated bucky unit for flat panel general radiography and fluoroscopy.
X-Ray TUBE	
Total of two numbers X Ray tubes, one is under couch and second ceiling mounted	

Ajay Kumar jineesh valakada Pushpinder Singh Khera Raju Sharma

•	The X-Ray tube should have dual focal spots.
•	X-Ray tube rating should be compatible with X-ray generator output.
•	Small focal spot power rating should be in the range 20-50 Kw.
•	Large focal spot power rating should be in the range 50-80 kW.
•	Size of focal spots should be specified.
•	Anode heat storage capacity should be 700 KHU or more.
•	Mention the heat dissipation rate.
Integrated Direct Digital Imaging system for Fluoroscopy:	
1.	Field of view of at least 40 cms or more.
2.	Collimator may be rectangular or iris type. Radiation free collimation should be possible.
3.	System should have real time optimization techniques to maintain constant brightness at the lowest allowances dose to the patient.
4.	Should have Cine loop facility and last image hold facility during fluoroscopy.
5.	System should be capable of acquiring images in the 2Kx2K matrix.
6.	The pulsed fluoroscopy mode - it should be at least 30 frames per second; and series exposures should be at least 6 frames per second.
Imaging Tower : Following are expected specifications for imaging tower. Please specify details in the quoted model :	
a)	Source-image distance (SID): min 89cms, max125 cm.
b)	Motor-assisted, 22 cm transverse travel, 14 cm to the front and back.
c)	Grip handle: Ergonomically shaped handle for one-handed control of main functions, Including force sensor-control of motorized tower movement, 8-way tabletop travel, table tilt, collimation control, acquisition trigger and fluoroscopy release.
d)	System should have provision for collision protection
Bucky wall stand :	
a)	Travel range (central beam to floor) From 30 cm to 173 cm.
b)	Detector unit Tiltable from – 20° to + 90°
c)	Alignment with X-ray tube.

jineesh valakada Pushpinder Singh Khera Raju Sharma

d)	Hand-held control: Tube tracking on/off and other important functions on user interface should be available.
e)	Tube automatically tracks wall Bucky height adjustments with detector tray height adjustments with detector at 0°, 90° or intermediate tilt angles.
f)	Suitable Grid of ratio 12:1 or better to be provided.
Detector System:	
a)	Wireless Digital flat panel detector over the table of size at least 43x43 cms or more.
1.	Image matrix size 2k X 2K pixels or more.
2.	Pixels size should be 150 micron or less.
3.	Should allow centered/de-centered collimation.
4.	DQE 70% or more.
5.	Tabletop to imaging tower distance adjustable in order to minimize radiation dose to the patient.
6.	Imaging tower movement should be motorized.
Image display system	
•	Flat medical grade monitors of 19" or more (four in number) to be provided of 1 Megapixel or more, two each in examination and console room.
•	Post acquisition image processing, viewing, reprocessing, hard copy documentation and onward transmission should be possible.
Control Console	
1.	All system movements of the table shall be controlled by the operator at the table in the examination room.
2.	The system should have facilities for edge enhancement, positive/negative image display, windowing, contrast/brightness, electronic shuttering, vertical and horizontal image reversal, and zoom functions.
3.	The system should have fast and direct access to all series, single images, in both examination (Remote controlled) and console room.
4.	System should have angle/distance measurement, image labeling and patient positioning facilities.
5.	System should have anon line dosimeter on the console to display actual radiation dose.
Image storage and Transmission	
•	Image storage capacity of at least 30,000 images in 1024 x 1024 matrix at 10/12 bits on the main system disk.
•	The system should be DICOM 3.0 (or higher version) ready (like send, receive, print, record on CD/DVD, acknowledge etc.) for connectivity to any network, computer/PC etc. in DICOM format.
•	Vendor should connect this with existing PACS system and other laser cameras already existing in the department without any extra

Atin Kumar

jineesh valakada

Pushpinder Singh Khera

Raju Sharma

	cost
•	Integration and networking will be done by the vendor free of cost with any other existing/future networking including other modalities, HIS and RIS and PACS.
Accessories	
1.	One Dry Chemistry, Multiport, multiple films (14"x 17", 11"X 14" and 8"X 10") camera with resolution of 500 DPI or more, DICOM ready and online. At least three size film trays should be active. The vendor should connect this camera with other existing cameras in department of Radiodiagnosis.
2.	Lead glass 100 x 150 cm for the console room.
3.	Five lightweight 'zero lead' aprons with integrated thyroid collar, pediatric gonadal shields (All sizes both for male and female). Stand to keep these aprons.
4.	Suitable UPS with complete backup for the computer system for at least 30 minutes.
5.	A voltage stabilizer of 120 KV or better for the entire unit.
6.	Minimum necessary furniture: chairs (rotating type computer chairs of reputed brand like Godrej) - 8 in number, table, shelves for storage space etc.
7.	Fire extinguisher alarm system to be connected to the nearest central system of the hospital by vendor.
8.	Hand grip
9.	Foot step.
10.	Patient fixing belts and compression device (for performing excretory urography).
11.	Integration with existing RIS & PACS to be done by the vendor free of cost.
Essential requirement :	
	The company should be ISO 13485 /CDESCO / FDA / European CE certified.
	The unit should be approved by AERB.
	The company should have a proven track record in the Govt. sector.
	At least two of the three components (generator, detector & X ray tube) should be from the same principal manufacturer of the X-ray system.
	During the CMC period, the QA for the unit must be done by the supplier as per AERB requirements.
	The company is to give an undertaking that the detector will be replaced with the same detector that was quoted during the initial offer for the entire warranty period and the CMC period. No change in the detector company is acceptable in case of replacement during the warranty /CMC period.

jineesh valakada

Pushpinder Singh Khera

Raju Sharma

DIGITAL RADIOGRAPHY SYSTEM (1000 mA) WITH WIRELESS DUAL FLAT PANEL DETECTOR (MID END)

The system should be capable of performing exposure in vertical, horizontal, and oblique positions to perform all skeleton body (upright and lying down) radiographs.

The unit should be completely integrated (integrated generator and Image acquisition). It should be possible to do all the general radiological imaging like abdomen, musculoskeletal, PNS, Skull, Spine, etc. with the movement of tube assembly with auto-positioning and auto-tracking.

The unit should be of High-frequency Digital Radiography system with a rotating anode. 3D ceiling suspended stand with Auto-tracking & 2 separate wireless detectors each in table bucky and vertical bucky.

The system should have the following features.

A. HIGH-FREQUENCY GENERATOR:

The generator should be of the latest technology with a high frequency.
Power output of 80KW.
KV range should be 40 to 150 KV in 1KV/step.
mA output: up to 1000 mA.
mAs range should be from 1 to 200 mAs.
It should have a solid-state automatic exposure control device on the table & vertical bucky stand with 3 AEC field sensors each on the table and wall stand .

B. X-RAY TUBE:

A Dual focus High-speed Rotating anode X-ray tube.
The focal spots of the tube should be:

- Small focus: 0.6
- Large focus: 1.2

Anode Heat storage capacity 300 KHU.
Collimator: Automatic Multileaf collimator with LED light source with high lux output. Rotation +/-90 degrees.
A DAP meter should be provided to display the dose given to the patient on the monitor.

C. TUBE STAND:

- Ceiling-mounted tube assembly with 3-dimensional motorized movements of the tube head covering a large area.
- Motorized movements in longitudinal, vertical, and transverse directions with control from panel mounted on Tube collimator assembly.
- Tube stands with actuator based/ telescopic noiseless swift motorized up/down movement.
- Manual Override of Longitudinal & Transverse direction movements with electromagnet locks

- Touch screen Console panel is provided for Exposure parameters display, tube inclination angle & SID display.
- A Smart Anti-collision software system is provided to avoid any collision.

Movements of the stand should be:

- Motorized Longitudinal movement: more than 2500 mm
- Motorized Transverse movement: more than 1500mm
- Motorized Vertical up/down movement: more than 1000mm
- Tube head Rotation (along the vertical axis): ±180°.
- Tube head Rotation (along the horizontal axis): ±135°.
- Tube assembly should have 3D auto-tracking and auto-positioning on its control for synchronization with the detector fitted inside the vertical bucky stand & table.
- Image stitching facility should be available in both vertical stand and table

D. TABLE:

- A horizontal 6-way table with a floating tabletop and adjustable height should be provided. Table-top should have three-dimensional movement, which is easy for patients as it lowers down to a comfortable position.
- The table should be provided with a motorized Bucky which can house the removable wireless detector
- Transverse and longitudinal movements of the tabletop should be locked by electromagnetic locks.
- A table should have up/ down motorized movement and it should be controlled by two up & down foot switches.
- Movements of table: Transverse movements - 18cm or more, longitudinal movements - 50cm or more. A height adjustment facility should be available.
- The maximum weight carrying capacity for the table during up/down movement should be more than 200 Kg.
- AEC mode with the use of ion chambers should be provided which enables auto selection of radiographic factors, saves time, eliminates retake, increases diagnostic capability and lowers radiation dose, calibrated to multiple exposure classes/densities.
- Removable grid of min 10:1 ratio with focal distance of 100 cm /110cms to be provided.

E. VERTICAL BUCKY (VB) STAND:

The floor-mounted Motorized Vertical bucky stand should house the removable wireless detector. It should have a user-friendly design and handling.

- VB stand should have provision to do chest radiography with and without a grid.
- Motorized Tilting should be -30 degrees to + 90 degrees.
- Vertical up & Down Movement range should be 1500mm or more.
- The vertical travel range of the detector should minimum 300 mm and maximum 1800 mm above floor (measured at the detector center).
- AEC mode with use of ion chambers should be provided which enables auto selection of radiographic factors, saves time, eliminates retake, increases diagnostic capability and lowers radiation dose, calibrated to multiple exposure classes/densities.
- Removable grid of min 10:1 ratio with focal distance of 100cm /110cms to be provided.

jineesh valakada Pushpinder Singh Khera Raju Sharma

F. FLAT PANEL DETECTOR (One NO. EACH FOR TABLE BUCKY AND VERTICAL BUCKY):

The wireless detector should be a flat panel type with A-Si (amorphous silicon) and CSi as scintillator.

- The size of the detector must be 43cm x 43cm.
- Active Image matrix 3K x 3K.
- Image depth should be 14 bits or more.
- Pixel size should be less than 150 um (Smaller pixel size is preferred)
- Detector resolution should be 3.6lp/mm or better.
- DQE (Detector Quantum Efficiency) should be more than 70%.

G: OPERATING STATION/WORKSTATION:

a. X-RAY/IMAGE CONTROL CONSOLE

Fully integrated system with the following features:

- Digital Display of KV & mAs.
- KV & mAs increase and decrease control on GUI
- Ready and X-Ray ON indication on GUI
- Self-diagnostic Program which can diagnose and display error messages such as Earth fault error, KV error, Filament error & Tube's Thermal Overload.
- Anatomical Programming Radiography (i.e. APR): Preprogrammed parameters of human Anatomy which helps the user to select exposure parameters based on body part, examination view and size of the patient should be available. Since it is a computer-based system (full system integration) so any number of Organ programming combinations should be possible. The user can define his own Organ parameters and can edit the existing parameters to his satisfaction and comfort level.
- APR programs: should be more than 1000 programs. (Expandable as per user's requirement).
- Hand switch with retractable cord for initiating the exposure for performing radiography procedures.

H. Workstation along with monitor: 2 No. 19" or more high-resolution LCD monitor should be provided with the specifications below.

Hardware Detail of Acquisition /Memory software:

- Compatible computer processor (i5 processor or Xeon Processor) of branded make
- 1TB Hard disk
- Window OS
- 64 Bit operating system
- CD/DVD writer.
- Wired keyboard & mouse.
- Operating system Windows 10 Pro operating system. Should be the latest version of Windows that the system can support. Any updates/upgrades/patches to the OS and the application should be provided free of cost for the entire period of warranty and CAMC.
- It is the vendors responsibility to connect the system to the closest network switch in the hospital network and to configure the system with HIS/RIS/PACS.

jineesh vatakada Pushpinder Singh Khera Raju Sharma

- It is the responsibility of the vendor to install a fire alarm system and connect it to the nearest available fire alarm panel, if such a system is available in the hospital. Else, the vendor has to install a standalone fire alarm and fighting system.
- Facility to transfer DICOM images in bulk to external hard disk is to be provided
- The workstation should have a DVD writer for burning images

I. POWER SUPPLY REQUIREMENT: 3 Phase, 400 Volts AC 50Hz with line resist 0.2 Ohms. Line Regulation ±10%.

J. Accessories: -

1. Four nos lead aprons of 0.5 mm lead equivalence.
2. Three-panel lead protection barrier.
3. Support stand for Image stitching radiography.
4. 3 KVA UPS for the console workstation with 30-minute backup to be provided
5. 3 tray Dry laser Printer to be supplied (at least 500 dpi)
6. Adequate thickness lead glass should be provided between the console room and the examination room

K. Other Requirements:

- The company should be ISO/ CDESCO/European CE/ FDA certified.
- The unit should be approved by AERB.
- The company should have a proven track record in the Govt. sector.
- During the CMC period, the QA for the unit must be done by the supplier as per AERB requirements.
- The company is to give an undertaking that the detector will be replaced with the same detector that was quoted during the initial offer for the entire warranty period and the CMC period. No change in the detector company is acceptable in case of replacement during the warranty /CMC period.
- Detector batteries, UPS and its batteries and all accessories supplied with the unit should be covered under warranty and CAMC

jineesh vatakada Pushpinder Singh Khera Raju Sharma

SPECIFICATIONS OF HIGH-FREQUENCY OVER THE COUCH DIGITAL R/F SYSTEM

Digital Radiography/Fluoroscopy System with Wireless Flat Panel Detector in remote-controlled RF table. The unit should be capable of doing all types of Fluoroscopic examinations like GI examination, ERCP, and barium studies, along with all radiography procedures.

X-RAY GENERATOR:

- A High-Frequency X-ray generator of frequency should be provided.
- The power output of the generator should be 80KW.
- KV Range should be:
  - Radiographic KV: 40 to 150 KV.
  - Fluoroscopic KV: 40 to 120 KV.
- mA Range (Rad.): 1000mA.
- mA Range (Fluoroscopy): Normal Flr. Mode: - up to 50mA
  HD/Boost Flouro/Cine mode: - up to 70mA.
- Exposure time (Rad.): 1 ms to 5 sec or more.
- Cumulative flouro. timer to cut off exposure.
- mAs Range (Rad.): up to 350mAs or more.

CONTROL:

Fully integrated system with the following features:

- Digital Display kV, mA & mAs for radiography & kV & mA for fluoroscopy mode, Cine kV & mA, Spot kV and mAs.
- Integrated touch panel TFT display for various X-ray functions and indications.
- Exposure parameters (eg. kV, mA, mAs) can be controlled from Acquisition software as well as from Touch Panel Display.
- Manual and Automatic brightness stabilization (ABS) in fluoroscopic Modes.
- Exposure indication on Acquisition Software.
- Self-diagnostic Program with Indicators for Earth fault error, kV error, Filament error & Tube's Thermal Overload, Rotor fault, and Phase failure indications.
- Anatomical Programming Radiography (i.e. APR) Preprogrammed parameters of human Anatomy > 150 programs which help the user to select exposure parameters based on the body part, examination view, and size of the patient.
- Hand switch with retractable cord for initiating the exposure for performing radiography procedures.
- 2-Point mode and 3-point mode exposure technique in Radiography mode.

X-RAY TUBE (01No.):

- A Dual focus Rotating Anode X-ray tube thermally protected having focal spots of 0.6 & 1.2mm.
- Anode rotation speed should be a minimum of 9000 RPM.
- The anode heat storage capacity of the tube should be min 1000KHU.
- One Pair of H.V. Cable of suitable length should be provided.

COLLIMATOR:

- 1No. Motorized Square/ Rectangular collimator having a bright light source and auto shut provision of the light.

TABLE:

Remote controlled, motorized RF Table should be provided. The table should have an integrated console. The table should have a scratch-resistant tabletop.

- The table should have a soft start and stop movement with the following minimum features.
- Motorized Tilt: Vertical +90° to -21° or more for Trendelenberg.

- The table should have an automatic stop at Horizontal & Vertical positions during tilt movement.
- Motorized Transverse movement of tabletop: 34cm or more
- Table with height adjustment facility
- Motorized Longitudinal movements of imaging unit i.e. Tube column – detector movement: 100cm or more with auto tracking facility
- Tube Oblique movement.
- Integrated bucky for wireless flat panel detector for general radiography and fluoroscopy.
- Remotely operated compression device.
- Footswitch for releasing fluoroscopy and acquisition.
- Patient weight carrying capacity: 200kg.
- Intercom system to communicate with the patients.
- The table and tube should be capable of performing chest radiography at an appropriate SID
- Table accessories: 1No. Each Handgrip, compression band, and footrest.

BUCKY WALL STAND:

- Travel range (central beam to floor) From 30 cm to 173 cm.
- Detector unit Tiltable from – 20° to + 90°
- Alignment with X-ray tube - Autotracking facility.
- Hand-held control: Tube tracking and other important functions on the user interface should be available.
- Tube automatically tracks wall Bucky height adjustments with detector tray height adjustments with the detector at 0°, 90°, or intermediate tilt angles.
- Suitable Grid of ratio 12:1 or better to be provided.
- The vertical travel range of the detector should be 1500 mm, minimum 300 mm and maximum 1800 mm above floor (measured at the detector center).

DYNAMIC FLAT PANEL DETECTOR (FPD) (2 No, one for table bucky and another for wall stand bucky

A complete imaging solution with cutting edge performance integrated with our X-ray systems.

FPD should have the following specifications or better.

- Receptor type: Amorphous Silicon
- Scintillator: Cesium iodide (CsI)
- Size of detector: 43 x 43cm or more
- Image matrix size: 3K x 3K or more
- A/D conversion: 16bits
- Pixel size:150µm or less.
- Detector resolution should be 3.6lp/mm.
- DQE: 70% or more at 0 lp/mm.

IMAGE ACQUISITION SOFTWARE should have the following features available.

Exposure Mode	• RF (For Fluoro, Cine and Spot) • DX (For Radiography)
Image Size/ Frame Rate	• RF: 1536×1536 (1.5K×1.5K Image resolution) Up-to 18 FPS Pulsed X-Ray • DX: 3072×3072 (3K×3K Image resolution)
Software Module	• Patient Entry Module: MWL, Manual, Emergency • Examination Module: - □ RF Module □ DX Module

	• Viewing Module • Print Module
Generator Controls feature in the software	• kVp • mAs • ABS ON/OFF • Filament Selection • Heat Unit Display • 3Point (KV, mA, mAs) / 2Point (KV, mAs)
Examination Layout	• 1x1 (Live) • 1x2 (1st: Live, 2nd: Reference)
Live Parameters	• WW/WL • Auto WW/WL • Dynamic Zoom • PAN • Horizontal Flip • Vertical Flip • Frame Rate • Image Invert • Image Rotation +90° • Image Rotation -90° • Software Shuttering/Live Image Masking
DICOM Compatibility	• DICOM 3.0 compatible: • DICOM Send • DICOM Print • DICOM MWL • DICOM MPPS
WL/WW Adjustment	• Automatic WW/WL adjustment for Radiography. • Automatic WW/WL adjustment for Fluoro, Cine, and Spot according to the selected procedures • Manual WL/WW adjustment
Post-processing Parameters	• WW/WL • Zoom • Magnify • Invert • Flip Horizontal • Flip Vertical • Annotations • Image Layouts • Series Layout • Image Cropping • Play DICOM Loops • Frame by Frame Image View • Software Shutter • Tagging of Images • Angle and Length measurement. • Image Reset

MONITORS: 2 Nos. medical grade monitors. of the size of 19" or more, one in the examination room integrated on the trolley and one in the console room with a resolution of 1280 x 1024 pixels or more should be provided.

File No. Z-28016/35/2024-PMSSY-IV (Computer No. 8285627)
Generated from eOffice by SARITA, EA(S)-PMSSY, DEO, DOHFW DEPARTMENT on 21/08/2024 05:43 pm

Raju Sharma

Additional reporting workstation with a 19" Medical display monitor with the below feature should be provided.

- Operating system Windows 10 Pro operating system. Should be the latest version of Windows that the system can support. Any updates/upgrades/patches to the OS and the application should be provided free of cost for the entire period of warranty and CAMC.
- It is the vendor's responsibility to connect the system to the closest network switch in the hospital network and to configure the system with HIS/RIS/PACS.
- Facility to transfer DICOM images in bulk to external hard disk is to be provided
- The workstation should have a DVD writer for burning images

Advance Features: -

- DICOM Store
- DICOM Print
- Job Queue

POWER REQUIREMENT: The unit should be operable on 400V AC, 50 HZ 3 Phase – Max. Allowable line Regulation ± 10%.

ACCESSORY:

- A servo voltage stabilizer of suitable rating for the complete unit.
- 30-minute UPS backup for the entire system including the x-ray tube, generator, table, and console to be provided
- 1 no dry laser printer of 500 DPI or more.
- 1 no. ceiling suspended lead protection shield.
- Lead glass should be provided for the console
- It is the responsibility of the vendor to install a fire alarm system and connect it to the nearest available fire alarm panel if such a system is available in the hospital. Else, the vendor has to install a standalone fire alarm and fighting system.

OTHER REQUIREMENTS:

- The company should be ISO 13485 / CDESCO / FDA / European CE certified.
- The unit should be approved by AERB.
- The company should have a proven track record in the Govt. sector.
- Out of the three components (generator, detector & x-ray tube) two should be from the same principal manufacturer of the X-ray system.
- During the CMC period, the QA for the unit must be done by the supplier as per AERB requirements.
- The company is to give an undertaking that the detector will be replaced with the same detector that was quoted during the initial offer for the entire warranty period and the CMC period. No change in detector company is acceptable in case of replacement during the warranty /CMC period.
- Detector batteries, UPS and its batteries and all accessories supplied with the unit should be covered under warranty and CAMC

Raju Sharma

SPECIFICATIONS FOR DIGITAL MOBILE DIGITAL RADIOGRAPHY UNIT (MID END)

A High-powered motorized battery-powered mobile Digital X-ray unit with a collapsible column and Telescopic Cross Arm suitable for bedside X-rays in Wards, ICUs, and operation theaters with a digital flat panel detector for image acquisition and should operate on single phase power supply. The quoted unit should have the following minimum specifications and items as mentioned below

The unit should comprise of the following:

I. High-Frequency Generator built into the mobile unit
II. X-Ray Tube
III. Collimator
IV. Flat Panel Detectors- 1no
V. Build in Workstation
VI. Integrated Mobile Cart

A. High Frequency Generator

1. It should be a microprocessor-controlled high-frequency X-ray generator
2. The power output of the generator should be 30KW or more to give at least 300mA@100kvP or more.
3. The radiographic KV range should be 40 KV to 125 KV or more with an increment of 1KV per step
4. mA Range: 10- 300 mA or more.
5. mAs Range: 0.1 to 300mAs
6. Exposure time – 1 ms to 10 Sec.
7. It should have a digital display of kVp, mA, and mAs
8. Individual settings of kVp, mA, mAs, and sec must be possible.
9. Wired as well as Wireless Exposure Switch to be provided

B. X-Ray Tube:

10. X-ray tube must have a rotating anode type with 3000 rpm or more.
11. Dual Focal Spot X-ray tube with 0.6mm for small focus and 1.5mm for large focus.
12. Tube Output should match the output of the Generator.
13. The anode heat storage capacity should be 200 KHU or more.

C. Collimator

14. The Tube unit should be fitted with a manual collimator with 2-axis blade control.
15. Should have the capability to select the additional copper filters of 0.1,0.2 and 0.3mm
16. Should have bright light preferably LED with minimum luminance of 160 lux or more
17. The collimator must be capable of rotating from -90 degrees to 180 degrees
18. Measuring tape to be provided

D. Flat Panel Detector:

19. The Wireless flat panel detector with CsI scintillator and amorphous Silicon of size at least 14" x 17"
20. The Scintillator must be on the exposure side facing the X-ray tube
21. The detector pixel matrix should be 2.5K x 3K or more
22. Pixel size should be 150 µm or Less
23. DQE of the detector must be 65% or more at 0 lp/mm
24. The image processing time after exposure should not be more than 7 sec.
25. The weight of the detector should not be more than 4kg.
26. The detector battery should be removable Li-Ion rechargeable type and least One additional Battery to be provided and provision of charging the battery within the unit.
27. The detector should be able to do a minimum of 200 X-rays on full charge.
28. The detector should be dust and waterproof with an IP54 rating

E. Integrated workstation and Control Panel:

29. The machine should have an integrated console with a touchscreen of size of min 21 inches or more

30. The processor should be i3 or better with min 16GB RAM and the latest Solid State Hard Disk of 500GB capacity.
31. The monitor should have a minimum 1.3 Mega Pixel resolution with full HD
32. The following Features should be available on the Control Panel
    a. Machine ON / OFF switch
    b. Digital Display of KV, mA, mAs and Sec
    c. kV, mA, and mAs increase and decrease switches
    d. Anatomical Programming should be provided in which kV and mAs are automatically selected depending upon the part of the body to be X-rayed
    e. Should be capable of storing user-defined APR setting
33. A detachable exposure switch with a cord of at least 5 m in length should be provided in addition to the exposure switch in the console. A remote-controlled exposure switch with a range of 5 m or more should also be provided
34. The console should be able to view the image and provide post-processing features using the touch screen.
35. The post-processing features should have zoom contrast and brightness adjustment, window, Level, etc.
36. The workstation should have image storage memory of at least 6000 images or more
37. The unit should have a facility for pediatric exposure management
38. The workstation software should support the following
    a. Patient List with the capability of DICOM worklist Query / Search on a variety of patient demographics
    b. Connectivity to DICOM printers with multi-format options for printing and to external storage devices and the DICOM network
    c. The machine should be fully network-ready and it should be possible to transfer images and patient data from and to the hospital network using LAN connectivity or Wireless LAN.

F. Mobile Cart Unit:

39. The entire system including the X-ray Generator, Tube, workstation console, Battery unit, and Column must be integrated as one single unit mounted on wheels on a mobile cart.
40. The Unit must have a collapsible column with a telescopic cross-arm
41. The Unit should be powered by a single Lithium Ion/ Polymer Battery for both movement and Exposure
42. The battery should provide power for the motor to move the machine with a driving speed of 5km/hr and capable of being moved along a slope of 5 degrees or more.
43. The machine should be able to do a minimum of 200 X-rays or more per full battery charge and also capable of moving a minimum of 15 km.
44. The Mobile unit must have a detector storage compartment with padded lining with a locking facility
45. The unit must have collision sensors and an effective braking system for parking, transport, and emergency braking
46. The tube unit must be mounted on a telescopic cross arm with a collapsible fully counterbalanced Column unit with the following specs for maximum positioning flexibility in any patient position
    a. The column rotation is +/- 300 degrees.
    b. Tube Reach from the center of the column should be min 80 and max 135 cm
    c. Tube rotation along the arm axis must be +/- 180 degrees
    d. Tube rotation along the tube axis must be +90 to -30 degrees
47. All cables should be concealed in the arm system.
48. The total weight of the Machine should not be more than 400 Kgs
49. The Cart battery should be charged from a normal 15A, 220-240V single phase socket in less than 5 hours
50. Operating system Windows 10 Pro operating system. Should be the latest version of Windows that the system can support. Any updates/upgrades/patches to the OS and the application should be provided free of cost for the entire period of warranty and CAMC.
51. It is the vendor's responsibility to connect the system to the closest network switch in the hospital network and to configure the system with HIS/RIS/PACS.
52. Facility to transfer DICOM images in bulk to external hard disk is to be provided

53. The workstation should have a DVD writer for burning images
54. Lead Aprons:- 0.5 mm Lead equivalence-2 nos
55. Optional item: 3 tray Dry laser Printer to be supplied (at least 500 dpi)

G. Power Line Connection:
The unit should be able to operate on single phase power supply with a plug-in facility to any standard wall outlet with a line voltage of 150 to 240V, 15AMP plug

Regulatory and Other Requirements

1. The whole unit should meet European CE / US FDA / CDESCO / BIS-approved
2. The unit quoted must have valid AERB type approval and NOC not accepted.
3. All Technical information in the tender document must be supported by original product data sheets.
4. Compliance sheets must strictly mention the reference pages of the datasheet
5. The company is to give an undertaking that the detector will be replaced with the same detector that was quoted during the initial offer for the entire warranty period and the CMC period. No change in detector company is acceptable in case of replacement during the warranty /CMC period.
6. Detector batteries, UPS and its batteries and all accessories supplied with the unit should be covered under warranty and CAMC

jineesh valakada Pushpinder Singh Khera Raju Sharma

TECHNICAL SPECIFICATION OF MOBILE DR (LOW END)

High-frequency Mobile Digital Radiography machine with a touch screen tablet & a portable WI-FI flat panel detector of size 35 cm X 43 cm (14" X 17")

- It should be a lightweight machine that allows the user easy maneuverability in congested areas of wards, ICU, or hospital/clinic. It should have an ergonomic articulated spring balanced tube stand allowing the operator to position the tube to acquire the images of desired views in patients positioned on standard ICU cots.
- Integrated Touch screen control panel for instant review of image, the size of the LCD/LED touch control panel should be more than 18".
- X-ray exposure parameter to be controlled from a touch screen control panel/workstation. The exposure parameters should be selected from the software and the details of radiographic parameters like KV and mAS should be tagged in the final image output.
- Single foot lock for wheel locking while movement.

GENERATOR & TUBE

X-Ray Generator Type	High-frequency microprocessor-controlled
Power Output	4 KW or more
Generator Frequency	110 Khz
KV Range	40 to 120 KV in 1 KV/step.
Maximum mA	110 mA.
mAs Range	1-320 mAs

Dual action hand switch & IR remote for ready & Exposure should be provided in addition to the console exposure switch. An emergency switch should be provided.

X-Ray Tube Head:-

Mono-block version x-ray tube head should be provided. The mono-block should consist of an X-ray tube, H.V. transformer, filament transformer, H.V. rectifiers, and capacitors, all immersed in high-grade oil with high dielectric strength. Mono-block Tube Head should be Protected from thermal overload.

Anode type	Stationary Anode
Focal Spot	1.8 mm
Heat Storage Capacity	42 KHU

FLAT PANEL DETECTOR (Wi fi)

Conversion screen/ Scintillator	Cesium Iodide (CsI)
Photodiode	amorphous silicon (a-si)
Size	43cm x 35cm
Active Image Matrix	3000x2400 or better
Pixel pitch	Less than 150µm
DQE	DQE @ 0lp/mm -70.%,
Grey Scale resolution, bits/pixel	14 bit
Weight of the detector	Less than 3.2 kgs
Image storage in FPD	up to 100 Images

IMAGING SOFTWARE

File No. Z-28016/35/2024-PMSSY-IV (Computer No. 8285627)
Generated from eOffice by SARITA, EA(S)-PMSSY, DEO, DOHFW DEPARTMENT on 21/08/2024 05:43 pm

Image Acquisition Software:

Integrated Image Software should provide complete control of all image capture functions & Exposure parameters control within the examination room. It should enhance the entire workflow by delivering diagnostic images instantly. It should allow the user to transfer X-Ray images electronically to remote workstations, image archives, and printers, also should have features such as:-

Software Features

1. **Main features**
- Patient Entry (Manual Emergency and MWL)
- Patient Search Based On PID, NAME, DAYS
- Exam window
- Process window
- View Window
- Print Window

2. **Post-processing features:-**
- WW/WL
- Rotate
- Zoom
- Flip
- Invert
- Annotations
- Measurements

3. **DICOM Compatible features:-**
- DICOM MWL
- DICOM print
- DICOM Send
- Operating system Windows 10 Pro operating system. Should be the latest version of Windows that the system can support. Any updates/upgrades/patches to the OS and the application should be provided free of cost for the entire period of warranty and CAMC.
- It is the vendor's responsibility to connect the system to the closest network switch in the hospital network and to configure the system with HIS/RIS/PACS.
- Facility to transfer DICOM images in bulk to external hard disk is to be provided
- The workstation should have a DVD writer for burning images

Tube Stand

The mobile stand offered should be a Spring balanced stand design which should fulfill stringent requirements of mobility, light in weight & easy maneuverability, and ease of operation. Mobile stand should be made to withstand all jerks while in use. Stand should be easily moved on the floor and a lock should be provided to lock the movement on the floor with the following details

- Vertical Travel of >1200mm
- Tube Head rotation of +/-90° along horizontal axis & +90° to -30° along tube axis
- The weight of the machine should be 150kgs or less
- Height should be 150 cm or less

Accessories

- Lead Aprons:- 0.5 mm Lead equivalence-2 nos.
- Inbuilt lead lined Detector storage box with padded lining ,with Lock and key facility for Detector safety.

- Optional item- 3 tray Dry laser Printer to be supplied (at least 500 dpi)

Power Supply:-

- 1-Phase 230V (AC-supply) 50/60 Hz, ±10% with automatic compensation
- 15 Ampere wall socket.
- The system should have an inbuilt battery for x-ray exposure in case of power failure. It should do a minimum of 50 X-rays per charge.

OTHER REQUIREMENTS:-

- The company should be ISO / EN-ISO / CDESCO/European CE / FDA certified.
- The unit should be approved by AERB.
- The system should be a fully integrated solution, retrofit type solution is not accepted.
- The company is to give an undertaking that the detector will be replaced with the same detector that was quoted during the initial offer for the entire warranty period and the CMC period. No change in detector company is acceptable in case of replacement during the warranty /CMC period.
- Detector batteries, UPS and its batteries and all accessories supplied with the unit should be covered under warranty and CAMC

Ajay Kumar jineesh valakada Pushpinder Singh Khera Raju Sharma

TECHNICAL SPECIFICATIONS FOR AI ENABLED DIGITAL FLAT PANEL DUAL DETECTOR 1000 MA X-RAY UNIT (HIGH END)

A high powered High-frequency Inverter technology, X-ray unit for general radiography with 2 nos wireless digital flat panels one in the vertical Bucky and the other in the table Bucky, having the capability to perform all the radiographic examination on both erect and supine positions with facility for Auto stitching on both the vertical and Table bucky and Auto Positioning facility. All software and stitching functionality should be from the OEM.

The unit should comprise of the following with the minimum specs as listed below:

I. Dual Flat Panel wireless detectors one for vertical and one for table exposures
II. High Frequency 80KW, 1000mA Generator
III. X-ray tube with Automatic Collimator
IV. Ceiling suspended unit with auto tracking and auto-positioning
V. Diagnostic X-ray table with auto-tracking
VI. Vertical Bucky Stand with auto-tracking
VII. Stitching Hardware for the vertical stitching.
VIII. Removable Grids for Vertical Bucky and Table Bucky
IX. Integrated X-Ray and DR console
X. Regulatory requirements

I. Wireless Flat Panel Detector (One on the wall stand and the other on the table):

The detectors should be able to perform all routine radiographic examinations. It should have the following features. The flat panel detector should be a proven technology with an amorphous silicon photodiode and CsI scintillator.

a) Wireless Flat Panel Detector with Tethering option with size of at least 43 cms x 43 cm for wall stand and table bucky
b) The detector should have a non-tiled CsI scintillator on the tube side and an amorphous silicon photodiode array behind it.
c) Image matrix size at least 3k x 3k
d) The minimum pixel size should be 150 microns or less.
e) Grey scale of 14 bits.
f) A/D conversion must be 14 bits minimum
g) Preview time after exposure 3 sec or less.
h) DQE at 0.0 lp/mm should be at least 70%
i) Spatial Resolution of 3.5 lp/mm or better
j) MTF of 80% @0.5 lp/mm
k) The detector should be dust and water-resistant with IP54 rating
l) Should have an inbuilt shock logging mechanism and data to be logged in the main console SW
m) The detector should be capable of swapping between vertical Bucky and Table Bucky
n) Modality workstation software with a direct registration facility for the CPU to be attached to the main console for the availability of multiple patient entries.

jineesh vatakada Pushpinder Singh Khera Raju Sharma

II. High-Frequency Generator

Microprocessor-controlled high-frequency X-ray Generator should be of the latest technology with constant output with low ripple frequency

a. Generator capacity must be 80 KW or more
b. KVP range 40 KV-150 KV
c. mA Output Should be 800mA @100 KV ; 1000 mA @80Kv or more
d. The generator frequency should be 450kHz or more
e. Exposure time should be 1 ms or 10 Sec.
f. The Generator capacity must be capable of giving 500mAs or more.
g. Automatic exposure control should be available with 3 AEC field sensors on the table and wall stand each.
h. Anatomical Protocol (APR) must be available and the user must be able to add any protocol that is needed
i. The generator must be completely integrated with the console workstation and it should be possible to control all exposure parameters from the software console.
j. Hand switch with retractable cord for initiating the exposure for performing radiography procedures.

III. X-Ray Tube & Collimator

The X-ray tube should be a high-speed rotating anode with dual focus, compatible with the generator capacity.

a. The Focal spot should be as below with the tube loading of
    i. Large Focal Spot 1.2mm x 1.2mm or less with loading of 96 Kw or more
    ii. Small Focal spot 0.6mm x 0.6mm or less with loading of 36 Kw or more
b. Anode heat storage capacity of 600 KHU or more.
c. Tube protection against overload should be available.
d. A high-speed rotor accelerator (starter) – minimum 8000 rpm
e. The collimator must be automatic with a manual override facility
f. It should be controllable by exam preset and control from the software
g. Collimator must be capable of rotation of +/- 45 deg or more
h. Must have laser centering and fitted with High luminance lamp
i. Blade control must be a 4-way motorized type with individual blade control
j. Should have motorized auto filter programmed with APR
k. Patient Dose Measurement should be possible using a DAP meter

IV. Ceiling Suspended 3D Column Stand with Display

a. Ceiling suspended tube with motorized adjustment should be provided with Horizontal and vertical auto-tracking of the tube and detector.
b. All movements should have electromagnetic brakes with fully counterbalanced mechanisms and should have sensors for collision protection
c. The tube should be capable of Auto Positioning based on the protocol setting
d. Movement in all directions should be easily possible.
e. Vertical telescopic movement should be at least 1500 mm.

f. The tube rotation must be ±120° or more.

g. The Tube Arm Rotation should be -150° to + 180° or more.

h. The Unit should have an LED /LCD display unit of a minimum of 9" size mounted on the tube side to display Positioning details such as SID, tube angle, etc. Additional information if displayed will be an added advantage.

i. Preview of the image to be displayed on the Tube Head Unit

j. Position of the detector angle to be displayed for correction of tube angle when the detector is out of the bucky

k. Should also be able to select the exposure parameters from the Tube head Unit

l. Motorized trans lateral movement using a remote control should be possible

V. X-Ray Table

a. 6 Way Fixed Table that has a motorized vertical Height adjustable and four-way floating table top fitted with a Flat detector of size at least 43x43cms with specification as mentioned in point 1., and has provision to rotate from landscape to portrait function without removing the detector.

b. Footswitch to be provided for all the movements.

c. The Table-top material should be made of low attenuation and durable to take the required patient weight.

d. The table should support a patient weight of at least 250 Kg.

e. It should be possible to synchronize detector movement with the movement of the X-ray tube. (Auto tracking)

f. Please specify the dimensions of the Table-top length and width

g. The table top movement should be (minimum) longitudinal movement: ± 40 cm, cross movement: ± 12 cm.

h. Longitudinal patient coverage should be 200cm or more without patient repositioning

i. It should have automatic grid sensing capability to avoid exposure with the wrong grid for patient safety.

j. A removable grid of min 10:1 ratio with a focal distance of 100 cm /110cms to be provided.

k. Auto stitching facility must be possible on the table bucky

VI. Vertical Bucky stand (wall Stand)

a. Motorized, counterbalanced, height adjustable vertical Bucky with a digital flat panel detector of size minimum 43 cms x 43 cms to be provided

b. It should be possible to synchronize detector movement with the movement of the X-Ray Tube. (Auto tracking)

c. Removable grid with grid of min 10:1 ratio and focus distance of 180cm to be provided

d. It should have automatic grid sensing capability to avoid exposure with the wrong grid for patient safety.

e. It should be possible to tilt the detector on the wall stand within a range of -20 to +90 degrees.

f. The detector holder must be possible to rotate by 45 degrees

g. The vertical travel range of the detector should be 1500 mm, a minimum of 300 mm, and a maximum of 1800 mm above the floor (measured center to center).

h. The Vertical Auto stitching must be available with the necessary stitching stand and accessories

File No.Z-28016/357/2024-PMSSY-IV (Computer No. 8285627)
Generated from eOffice by SARITA, EA(S)-PMSSY, DEO, DOHFW DEPARTMENT on 21/08/2024 05:43 pm Raju Sharma

7. Operating Station and Console

The operating console/workstation must be an integrated system to manage the patient information such as adding, editing, and deleting the patient information, Capturing and acquiring images, setting of the X-ray exposure parameters, managing and post-processing of the image using the software tools, and archiving of the images. The system also should be fully DICOM 3.0 compliant or above having the below specifications

a. Latest PC-based workstation of reputed brands like DELL or HP with latest intel based processor.
b. It should have SSD 256GB + HDD 1TB or more.
c. RAM of 16 GB or more to be provided
d. HDD encryption and cyber security protection are to be provided
e. 19-inch latest High-Quality LED monitor must be provided along with the console.
f. The console software must be able to manage the patient information and be capable of connecting to the RIS / HIS and PACS network.
g. X-ray parameters such as KVP, mA, mAs, X-ray procedure and protocol, AEC, Grid type, focal spot, etc. selection should be possible from the single console.
h. The console should display the wireless signal strength and the battery charge condition.
i. Should be able to show the image on the screen in less than 3 seconds after exposure for the preview of the image
j. The console software must provide a full range of post-processing features like Geometric Corrections, Window / Level, Algorithms, Annotations such as markers, predefined texts, drawing lines and geometrical shapes, measuring distances and angles, Cobb's Angle, Shuttering, histograms, Zoom, Grey Scale Reversal.
k. There should be a provision to display the virtual drawing of the receptor boundary and AEC chambers on the patient using a real-time camera should be possible.
l. Collimator shutters should be adjusted from the console software using a real-time camera function
m. There should be a provision to get the patient motion alarm in the console SW
n. Automatic Source tilting method Image Stitching Software up to 3 or 4 images must be provided for performing full leg full spine / long body imaging in both vertical bucky and table bucky
o. Scoliosis measurement and leg length difference measurement tools must be provided.
p. The console should also have the functionality/tool to correct radiographic magnification on the image
q. AI-based Scatter Reduction tool to be provided for removal of scatter Radiation in the image without the need for a physical grid
r. The Console system must be capable of advanced AI features such as Bone suppression imaging, identifying Lung nodules automatically in single exposure only and not multiple exposures. Also, the Post-processing to be part of the console software
s. The console should have an automatic program to indicate over /under exposure visually in the preview screen
t. The console system should have the functionality to automatically detect and correct the detector line artifact and can be accessed by the user.
u. The system should be fully DICOM 3.0 Ready
v. It should get the DICOM worklist from HIS/RIS, store images through the PACS network system, and support DICOM image print and DICOM MPPS functions.

8. Independent image viewing, Post Processing dicom workstation - 1 Nos.

File No.Z-28016/357/2024-PMSSY-IV (Computer No. 8285627)
Generated from eOffice by SARITA, EA(S)-PMSSY, DEO, DOHFW DEPARTMENT on 21/08/2024 05:43 pm

a. A post-processing workstation with a high-resolution medical-grade color monitor should be provided with the system
b. Graphics card: NVIDIA GeForce GTX 1050 Ti or better or better with 4GB DDR4 memory
c. Display 19" or more FHD medical-grade monitor
d. Processor intel i7 10th generation or better
e. RAM 16GB expandable up to 32GB
f. Storage Dual drives with 256GB Solid State Drive +1TB Hard Drive
g. Operating system Windows 10 Pro operating system. Should be the latest version of Windows that the system can support. Any updates/upgrades/patches to the OS and the application should be provided free of cost for the entire period of warranty and CAMC.
h. It is the vendor's responsibility to connect the system to the closest network switch in the hospital network and to configure the system with HIS/RIS/PACS.
i. It is the responsibility of the vendor to install a fire alarm system and connect it to the nearest available fire alarm panel if such a system is available in the hospital. Else, the vendor has to install a standalone fire alarm and fighting system.
j. Facility to transfer DICOM images in bulk to external hard disk is to be provided
k. The workstation should have a DVD writer for burning images
l. The workstation software should support the following:

    i. Patient List with the capability to query /search based on various criteria such as name, ID number, date of examination, etc.
    ii. Features such as DICOM Viewing, windowing, zoom Pan magnify Annotate, mark < measure, Reporting
    iii. Connectivity to DICOM printers with multi-format options to be provided
    iv. The workstation should be Dicom ready and have provision to connect to external storage devices and DICOM servers

Accessories

a. Voltage Stabilized of Suitable capacity for the entire system must be provided
b. 3 KVA UPS for the console workstation with 30-minute backup to be provided
c. Compression Belt and Patient Hand Grips are to be provided
d. 3 tray Dry laser Printer to be supplied (at least 500 dpi)

e. Adequate thickness lead glass should be provided between the console room and the examination room

a. Regulatory Approval and other requirements:

The Digital Radiography System offered should have the following:

I. The complete system should have US FDA/CDESCO/BIS/European CE approval
II. Valid AERB Type approval of the system quoted for installing the unit in India. NOC is not acceptable.

b. Room for installation to be inspected by the prospective bidders.
c. Two out of three components (tube, generator and detector) should be from the OEM
d. During the CMC period, the QA for the unit must be done by the supplier as per AERB requirements.

File No.Z-28016/357/2024-PMSSY-IV (Computer No. 8285627)
Generated from eOffice by SARITA, EA(S)-PMSSY, DEO, DOHFW DEPARTMENT on 21/08/2024 05:43 pm

e. The company is to give an undertaking that the detector will be replaced with the same detector that was quoted during the initial offer for the entire warranty period and the CMC period. No change in the detector company is acceptable in case of replacement during the warranty /CMC period.

f. Detector batteries, UPS and its batteries and all accessories supplied with the unit should be covered under warranty and CAMC

jineesh valakada | Pashpinder Singh Khera | Raju Sharma

TECHNICAL SPECIFICATIONS FOR DIGITAL FLAT PANEL DUAL DETECTOR 630 MA X-RAY UNIT (LOW END)

A High powered with High frequency Inverter technology, X-Ray Unit for general radiography with 2 nos wireless digital flat panels one in the vertical Bucky and the other in the table Bucky, having the capability to perform all the radiographic examination on both erect and supine position. The unit should comprise of the following with the minimum specs as listed below:

I. Dual Flat Panel wireless detectors one for vertical stand and one for table Bucky
II. High Frequency 50KW, 630mA Generator
III. X-Ray Tube with automatic Collimator
IV. Floor mounted unit
V. Diagnostic X-Ray Table
VI. Vertical Bucky Stand
VII. Removable Grids for Vertical Bucky and Table Bucky
VIII. Integrated X-Ray and DR console
IX. Regulatory requirements

I. Wireless Flat Panel Detector (One on the wall stand and the other on the table):

The detectors should be able to do all routine Radiographic examinations. It should have the following features. The flat panel detector should be of proven technology with amorphous silicon photodiode and CsI scintillator.

a) Wireless Flat Panel Detector with size of at least 43cm x 43cm for wall stand and table bucky
b) The detector should have a non-tiled CsI scintillator on the tube side and amorphous silicon photodiode array behind it.
c) Image matrix size at least 3k x 3k
d) Minimum pixel size should be 150 microns or less.
e) Grey scale of 14 bit.
f) A/D conversion must be 16 bits minimum
g) Preview time after exposure 5 sec or less.
h) DQE at 0.0 lp/mm should be at least 70%
i) Spatial Resolution of 3.5 lp/mm
j) MTF of 80% @0.5 lp/mm and above
k) Detector should be dust and water resistance with IP54 rating
l) Should have inbuilt shock logging mechanism and data to be logged in the main console
m) Detector should be capable of swapping between vertical Bucky and Table Bucky
n) Modality workstation software with direct registration facility to be attached to the main console for availability of multiple patient entries.

II. High Frequency Generator

Microprocessor controlled high frequency X-Ray Generator should be of latest technology with constant output with low ripple frequency

a. Generator capacity must be 50 KW or more
b. KVP range 40 KV-150 KV
c. Generator should be of high frequency
d. Exposure time should be 1 ms or 10 Sec.
e. Hand switch with retractable cord for initiating the exposure for performing radiography procedures.

File No.Z-28016/35/2024-PMSSY-IV (Computer No. 8285627)
Generated from eOffice by SARITA, EA(S)-PMSSY, DEO, DOHFW DEPARTMENT on 21/08/2024 05:43 pm

f. Automatic exposure control should be available with 3 AEC field sensors each on table and wall stand.
g. Anatomical Protocol (APR) must be available and user must be able to add any protocol which is needed
h. The generator must be completely integrated with the console workstation and it should be possible to control all exposure parameters from the software console.

III. X-Ray Tube & Collimator

The X-Ray Tube should be High speed rotating anode with dual focus, compatible with the generator capacity.

a. The Focal spot should be as below
    i. Large Focal Spot 1.2mm
    ii. Small Focal spot 0.6mm
b. Anode heat storage capacity of 300 KHU or more.
c. Tube protection against overload should be available.
d. Collimator must be automatic with manual override facility
e. Should be controllable by exam preset and control from the software
f. Collimator must be capable of rotation of +/- 45 deg or more
g. Must have laser centering and fitted with High luminance lamp
h. Blade control must be 4 way motorized type mapped with APR
i. Should have motorized auto filter programmed with APR
j. Patient Dose Measurement should be possible using DAP meter

IV. Floor mounted Column stand

a. Movement in all directions should be easily possible.
b. Vertical telescopic movement should be at least 1500 mm.
c. The tube rotation must be ±120° or more.
d. The Tube Arm Rotation should be -150° to + 180° or more

V. X-Ray Table

a. 6 Way Fixed Table which has motorized vertical Height adjustable and with four way floating table top fitted with Flat panel detector of size at least 43x43cms with specification as mentioned in point 1
b. Footswitch to be provided for all the movements.
c. The Table top material should be made of low attenuation and durable to take the required patient weight.
d. Table should support patient weight of at least 200 Kg.
e. Please specify the dimensions of Table top length and width
f. The table top movement in longitudinal direction (minimum) - ± 40 cm, cross movement: ± 12 cm.
g. Longitudinal patient coverage should be 200cm or more without patient repositioning
h. Removable grid of min 10:1 ratio with focal distance of 100 cm /110cms to be provided.

VI. Vertical Bucky stand (wall Stand)

a. Motorized, counter balanced, height adjustable vertical Bucky with a digital flat panel detector of size minimum 43 cms x 43 cms to be provided
b. Removable grid with grid of min 10:1 ratio and focus distance of 180cm to be provided
c. The vertical travel range of the detector should be 1500 mm, minimum 300 mm and maximum 1800 mm above floor (measured at the detector center).

7. Operating Station/ Console (2 sets)

The operating console / workstation must be an integrated system to manage the patient information such as adding, editing and deleting the patient information, Capturing and acquiring images, setting of the X-ray exposure parameters, managing and post processing of the image using the software tools and archiving of the images. The system also should be fully DICOM 3.0 compliant or above having the below specifications

a. Latest PC Based workstation of reputed brands like DELL or HP with latest intel based processor.
b. It should have the SSD storage of 256GB + HDD storage of 1TB or more.
c. RAM of 16 GB or more to be provided
d. HDD encryption and cyber security protection to be provided
e. 19 inches latest High Quality LED monitor must be provided along with the console.
f. The console software must be able to manage the patient information and capable of connecting to the RIS / HIS and PACS network.
g. The console should display the detector's wireless signal strength and the battery charge condition.
h. Should be able to show the image on the screen in less than 3 sec after exposure for the preview of the image
i. The console software must provide full range of post processing features like Geometric Corrections, Window / Level, Algorithms, Annotations such as markers, predefined texts, drawing lines and geometrical shapes, measuring distances and angles, cobb's Angle, Shuttering, Zoom, Grey Scale Reversal.
j. System should be fully DICOM 3.0 Ready
k. It should get DICOM worklist from HIS/RIS, store images through the PACS network system and should support DICOM image print and DICOM MPPS functions.
l. Operating system should be Windows 10 Pro. Should be the latest version of Windows that the system can support. Any updates/upgrades/patches to the OS and the application should be provided free of cost for the entire period of warranty and CAMC.
m. It is the vendors responsibility to connect the system to the closest network switch in the hospital network and to configure the system with HIS/RIS/PACS.
n. It is the responsibility of the vendor to install a fire alarm system and connect it to the nearest available fire alarm panel, if such a system is available in the hospital. Else, the vendor has to install a standalone fire alarm and fighting system.
o. Facility to transfer DICOM images in bulk to external hard disk is to be provided
p. The workstation should have a DVD writer for burning images
q. 3 KVA UPS for the console workstation with 30-minute backup to be provided
r. 3 tray Dry laser Printer to be supplied (at least 500 dpi)
s. Adequate thickness lead glass should be provided between the console room and the examination room

a. Regulatory Approval and other requirements:

The Digital Radiography System offered should have the following:

a. The complete system should have US FDA/ European CE/CDESCO/BIS approved
b. Room for installation to be inspected by the prospective bidders.
c. During the CMC period, the QA for the unit must be done by the supplier as per AERB requirements.
d. The company to give undertaking that the detector will be replaced with the same detector that was quoted during the initial offer for the entire warranty period and the CMC period. No change in detector company is acceptable in case of replacement during warranty /CAMC period.

File No.Z-28016/35/2024-PMSSY-IV (Computer No. 8285627)
Generated from eOffice by SARITA, EA(S)-PMSSY, DEO, DOHFW DEPARTMENT on 21/08/2024 05:43 pm

e. Detector batteries, UPS and its batteries and all accessories supplied with the unit should be covered under warranty and CAMC

Atin Kumar

Jineesh Valakada

Pushpender Singh Khera

Raju Sharma

SPECIFICATIONS FOR HIGH END DIGITAL MOBILE DIGITAL RADIOGRAPHY UNIT (HIGH END)

A High-powered motorized battery-powered mobile Digital X-ray unit with a collapsible column and Telescopic Cross Arm suitable for bedside X-rays in Wards, ICUs, and operation theaters with a digital flat panel for image acquisition and should operate on a single-phase power supply. All software functionality should be from the OEM.

The quoted unit should have the following minimum specifications and items as mentioned below

The unit should comprise of the following:

I. A High-Frequency Generator built into the mobile unit
II. X-Ray Tube
III. Collimator with Display Tube unit
IV. Flat Panel Detectors- 1no
V. Build in Workstation
VI. Integrated Mobile Cart

A. High Frequency Generator

1. It should be a microprocessor-controlled high-frequency X-ray generator
2. The power output of the generator should be 40KW or more to give at least 400mA@100kvP or more.
3. The radiographic KV range should be 40 KV to 150 KV or more with an increment of 1KV per step
4. mA Range: 10- 500 mA or more.
5. mAs Range: 0.1 to 500mAs
6. Exposure time – 1 ms to 10 Sec.
7. It should have a digital display of kVp, mA, and mAs
8. Individual settings of kVp, mA, mAs, and sec must be possible.
9. Wired as well as Wireless Exposure Switch to be provided in addition to the exposure switch in the console

B. X-Ray Tube:

10. X-ray tube must be with a rotating anode type with 3000 rpm or more.
11. Dual Focal Spot X-ray tube with 0.6mm for small focus and 1.2mm for large focus.
12. Tube Output should match the output of the Generator.
13. The anode heat storage capacity should be 300 KHU or more.

C. Collimator and display unit

14. The Tube unit should be fitted with Automatic collimator with individual Blade control and manual override
15. Should have the capability to select the additional filters automatically based on the APR
16. Copper filters of 0.1, 0.2, and 0.3 mm are to be provided
17. Should have bright light preferably LED with minimum luminance of 160 lux or more
18. The collimator must be capable of rotating from -90 degrees to 180 degrees
19. Measuring tape to be provided
20. At the tube side, there should be a 7" or more color touch panel which gives the details of tube angulation, X-ray selected parameters, distance, and all other vital information such as patient details.
21. Should also be able to select the Exposure parameters from the tube head unit
22. Preview of the image to be displayed in the Tube head unit
23. The position of the detector angle to be displayed for correction of the tube angle

D. Flat Panel Detector:

24. The Wireless flat panel detector with CsI scintillator and amorphous Silicon of size at least 14" x 17"
25. The Scintillator must be on the exposure side facing the X-ray tube
26. The detector pixel matrix should be 2.5K x 3K or more
27. Pixel size should be 150 µm or Less
28. DQE of the detector must be 70% or more at 0 lp/mm

File No.Z-28016/35/2024-PMSSY-IV (Computer No. 8285627)
Generated from eOffice by SARITA, EA(S)-PMSSY, DEO, DOHFW DEPARTMENT on 21/08/2024 05:43 pm Raju Sharma

29. The image processing time after exposure should not be more than 5 sec.
30. The weight of the detector should not be more than 3kg.
31. The Detector battery must be capable of getting charged in the storage compartment.
32. The detector battery should be removable Li-Ion rechargeable type and least One additional Battery to be provided and provision of charging the battery within the unit.
33. The detector should be able to do a minimum of 500 X-rays on a full charge.
34. The detector should be dust and water-resistant with an IP54 rating
35. The detector should have a minimum distributed weight-bearing capacity of 350kg and should have a minimum bend capacity of 100 kg.
36. Should have an inbuilt shock logging mechanism and data to be logged in the main console SW

E. Integrated workstation and Control Panel:

37. The machine should have an integrated console with a touchscreen of size of min 21 inches or more
38. The latest processor with min 16GB RAM and the latest Solid State Hard Disk of 1TB capacity.
39. The monitor should have a minimum 1.3 Mega Pixel resolution with full HD
40. The following Features should be available on the Control Panel
    a. Machine ON / OFF switch
    b. Digital Display of KV, mA, mAs and Sec
    c. kV, mA, and mAs increase and decrease switches
    d. Anatomical Programming should be provided in which kV and mAs are automatically selected depending upon the part of the body to be X-rayed
    e. Should be capable of storing user-defined APR setting
41. A detachable exposure switch with a cord of at least 5 m in length should be provided in addition to the exposure switch on the console.A remote-controlled exposure switch with a range of 5 m or more should also be provided
42. The console should be able to view the image and provide post-processing features using the touch screen.
43. The post-processing features should have zoom contrast and brightness adjustment, window, Level, etc.
44. Workstation should have image storage memory of at least 10000 images.
45. The unit should have a facility for pediatric exposure management
46. AI-based Scatter Radiation tool to be provided for removal of scatter Radiation in the image without the need for a physical grid and should be a part of main console software and can be mapped with APR
47. Dose measurement to be provided and also to be sent as a DICOM image to the PACS.
48. The Console system must be capable of advanced AI features such as Bone suppression imaging, identifying Lung nodules, Pneumothorax, and Pleural effusion automatically in single exposure only and not in multiple exposures. Also, the Post-processing should be part of the console software and can generate the findings automatically post-acquisition.
49. HDD encryption and cyber security protection are to be provided
50. Interactive Tube head unit with the function of minor adjustments to the motorized movement of the machine from the tube side must be possible
51. A laser-centering device for the accurate positioning of SID is to be provided and should be APR-based.
52. The workstation software should support the following
    a. Patient List with the capability of DICOM worklist Query / Search on a variety of patient demographics
    b. Connectivity to DICOM printers with multi-format options for printing and to external storage devices and the DICOM network
    c. The machine should be fully network-ready and it should be possible to transfer images and patient data from and to the hospital network using LAN connectivity or Wireless LAN.
    d. There should be a provision to access the RIS/PACS browser within the console SW

Pushpender Singh Khera Raju Sharma

53. Operating system Windows 10 Pro operating system. Should be the latest version of Windows that the system can support. Any updates/upgrades/patches to the OS and the application should be provided free of cost for the entire period of warranty and CAMC.

54. It is the vendor's responsibility to connect the system to the closest network switch in the hospital network and to configure the system with HIS/RIS/PACS.

55. Facility to transfer DICOM images in bulk to external hard disk is to be provided

56. The workstation should have a DVD writer for burning images

F. Mobile Cart Unit:

57. The entire system including the X-ray Generator, Tube, workstation console, Battery unit, and Column must be integrated as one single unit mounted on wheels on a mobile cart.
58. The Unit must have a collapsible column with a telescopic cross-arm
59. The Unit should be powered by a single Lithium Ion/ Polymer Battery for both movement and Exposure
60. The battery should provide power for the motor to move the machine with a driving speed of 5km/hr and capable of being moved along a slope of 5 degrees or more.
61. The machine should be able to do a minimum of 300 X-rays or more per full battery charge and also capable of moving a minimum of 30 km.
62. The Mobile unit must have a detector storage compartment with a charging facility and detector locking facility, unlocking of the Detector lock should be password protected, and a physical key is not accepted
63. The unit must have collision sensors and an effective braking system for parking, transport, and emergency braking
64. The tube unit must be mounted on a telescopic cross arm with a collapsible fully counterbalanced Column unit with the following specs for maximum positioning flexibility in any patient position
    a. The column rotation is +/- 300 degrees.
    b. Tube Reach from the center of the column should be min 80 and max 135 cm
    c. Tube rotation along the arm axis must be +/- 180 degrees
    d. Tube rotation along the tube axis must be +90 to -30degree
65. All cables should be concealed in the arm system.
66. The detector should be capable of charging automatically in the cabinet during movement.
67. The total weight of the Machine should not be more than 360 Kgs
68. The Cart battery should be charged from a normal 15A, 220-240V single phase socket in less than 5 hours
69. Lead Aprons:- 0.5 mm Lead equivalence-2 nos
70. Optional item - 3 tray Dry laser Printer to be supplied (at least 500 dpi)

G. Power Line Connection:

The unit should be able to operate on single phase power supply with a plug-in facility to any standard wall outlet with a line voltage of 150 to 240V, 15AMP plug

Regulatory and Other Requirements

1. The whole unit should meet European CE / US FDA /CDESCO /BIS-approved
2. The unit quoted must have valid AERB type approval and NOC not accepted.
3. All Technical information in the tender document must be supported by original product data sheets.
4. Compliance sheets must strictly mention the reference pages of the datasheet

5. The company is to give an undertaking that the detector will be replaced with the same detector that was quoted during the initial offer for the entire warranty period and the CMC period. No change in detector company is acceptable in case of replacement during the warranty /CMC period.

6. Detector batteries, UPS and its batteries and all accessories supplied with the unit should be covered under warranty and CAMC

jineesh valakada Pushpinder Singh Khera Raju Sharma

Specification for Mobile Flat Panel Detector C-Arm Unit (High end)	
	Mobile C-Arm with Flat Panel system with true counterbalanced C arm for fluoroscopic and X-ray operation.
A.	**Gantry / C-Arm**
	Fully counterbalanced C-arm with side-to-side (wig-wag) and horizontal travel movements, and the following features:
1	Motorized Angulations movement: at least 140 degrees or more.
2	Motorized longitudinal movement: at least 200 mm or more
3	Motorized Orbital Rotational Movement: at least 140 degrees or more
4	Motorized Vertical movement: at least 485 mm or more
5	Swivel range: ±10 degrees
6	Depth of immersion: 73 cm or more
7	source to image distance: 990 mm or more
8	Free space within the C-arm: at least 77 cm
9	Field of view: square field of view for better ROI coverage.
10	Touch-based panel for control of C-Arm functions mounted on the C-arm stand itself.
11	The collision prevention sensors help support patient safety by stopping the C-Arm Movement when an object is sensed/detected within the periphery of the detector.
B	**Generator & X-Ray Tube**
1	The generator should be a microprocessor-controlled converter & type with an output of at least 15 KW.
2	Modes: continuous, digital pulse fluoroscopy and digital radiography.
3	Fluoroscopic KVp range: 40-120kV, minimum 60 mA.
4	Radiographic kVp range: 40-120kVp, minimum 125 mA or more.
5	The X-ray tube should have a rotating anode.
6	Anode heat storage capacity should be 300 KHU or higher.
7	Anode cooling capacity should be 75 KHU /minute or higher.
8	Tube housing heat storage capacity should be a minimum of 2000 KHU.
9	The generator should provide digital pulse fluoroscopy with pulse rates of at least 15 frames/second.
10	Additional safety size filtration for the safety of scattered radiation
11	The focal spot size should be 0.3mm & 0.6mm dual focal spots.
12	Automatic dose rate control.
13	Integrated laser high localizer, radiation-free collimation
14	Multifunction foot switch to control all operating modes and single image storage out of the sterile field.
15	Inbuilt heat management capabilities for long interventional procedures.
16	Integrated dose monitoring chamber.
17	Metal Artifact reduction/metal correction should be available.
18	Additional safety size filtration should be 4 mm or more Al Equivalent
19	The system should have the Software facility to allow free positioning of the anatomy, even at the edge of the image detector. It automatically detects anatomy and adjusts parameters to produce high-quality images
C	**Flat Panel Detector System**
1	Flat detector of CSI (Cesium Iodide) with amorphous Silicon doping.
2	Size of detector: at least 30 X 30 cm or more
3	The pixel size should be 155 microns or less.
4	The resolution of the detector must be 1.5 K x 1.5 K.
5	Image inversion: right to left top to down
6	Provide a last image hold capability that the last image is displayed on the active monitor after the termination of exposure.

7	Cable-free rear side and 180-degree rotatable monitors.
8	Equipped with two high-resolution 19" HD LED/LCD/TFT monitors with Diagnostic Image quality with an image matrix of 1024 x 1024 or more in the exam room.
9	Vertically and horizontally adjustable monitor for specific needs.
10	Viewing angle of at least 150 degrees with the ergonomic mounting of the monitors on the mobile view station.
11	The system shall allow the user to change the image orientation on the display screen during a live exposure or using the last image hold. Those functions include image rotation, left-to-right, and top-bottom image reversals.
D	**Digital System & Image Management**
1	Multipatient database for handling large quantities of images, including dose management reports.
2	Automatically select proper Imaging parameters, kVp, and mA during an image, but also allow the user to override these settings manually.
3	Real-time and automatic brightness and contrast should be provided to optimize the displayed image.
4	Provide a real-time post-processing edge enhancement capability to get better image quality according to the density of the tissue. An electronic zoom function, an automatic save function to hard disk, Mosaic Display.
5	The system should save more than 1 lac image to the internal hard disk and retrieve stored images later.
6	It should have a facility to record online fluoroscopy.
7	Should have facility for image and Fluoro sequences retrieval on a CD/DVD/Pen drive and print Images on paper/ firm.
8	The system should have a facility for DICOM connectivity and DICOM ready (HIS compatible DICOM modality worklist, DICOM send/ receive, DICOM print, DICOM query retrieve). All DICOM functions should be offered and installed when needed at no additional cost.
9	Facility for wireless data transfer.
10	The System should be equipped with a touch control panel on the patient table side with a Preview image.
11	Position memory & position tracking.
12	The system must have a Sensor inside the Detector and non-touch Collision protection. It must have an automatic position Control Feature for C-arm positioning.
13	Operating system Windows 10 Pro operating system. Should be the latest version of Windows that the system can support. Any updates/upgrades/patches to the OS and the application should be provided free of cost for the entire period of warranty and CAMC
14	It is the vendor's responsibility to connect the system to the closest network switch in the hospital network and to configure the system with HIS/RIS/PACS
15	Optional Items: • 3 tray Dry laser Printer to be supplied (at least 500 dpi) • Software and hardware capability of performing digital subtraction angiography
E	**Essential Accessories.**
1	Suitable U.P.S online to run the entire system for at least 15 minutes of Backup time.
2	APRON ultra-lightweight: - 4 No.
3	Thyroid Shield - 04 nos., lead goggles 2
4	Sterile covers for C-Arm, X-ray tube, and flat panel detector (disposable):100 for each
6	Lead Apron Stand: - 01 nos.
7	Patient Table: Compatible, Free-floating, transparent to X-rays with motorized table movement (Cranio-caudal, left-right, up-down). Control Switch for table movement on the table itself.
H	**Terms & Conditions:**
1	The company should be ISO 13485 / ICMED / FDA / European CE certified.
2	During the CMC period, the QA for the unit must be done by the supplier as per AERB requirements.
3	The unit should be approved by AERB.
4	The company should have a proven track record in the Govt. sector.

5	Out of the three components (generator, detector & x-ray tube), two should be from the same principal manufacturer of the X-ray system
6	The company is to give an undertaking that the detector will be replaced with the same detector that was quoted during the initial offer for the entire warranty period and the CMC period. No change in detector company is acceptable in case of replacement during the warranty /CMC period

jineesh valakada Pushpinder Singh Khera Raju Sharma

Specification for Low end Mobile Flat Panel Detector C-Arm Unit (Low end)	
	Mobile C-Arm with Flat Panel system with true counterbalanced C arm for fluoroscopic and X-ray operation.
A.	**Gantry / C-Arm**
	Fully counterbalanced C-arm with side–to–side (wig-wag) and horizontal travel movements, and the following features:
1	Orbital rotation movement: +/- 200 deg or more
2	Angulation: at least:155° or more
3	Horizontal movement: more than 195 mm
4	Vertical movement: at least 49 cm motorized movement
5	Swivel range: ±10 degrees
6	Depth of immersion: 73 cm or more
7	Free space within the C-arm: at least 76 cm
8	Remote control (touch-based) for control of C-Arm functions.
9	Touch-based panel for control of C-Arm functions mounted on C-arm stand itself
10	The operator should be able to have control on his side
11	The system should have the capability of an electromagnetic locking system
12	The system should come with uniform reference for the operator and the physician to be used during the positioning of the C arm
B	**Generator & X-Ray Tube**
1	The generator should be a microprocessor-controlled converter & type with an output of at least 4 KW or more.
2	Modes: continuous, digital pulse fluoroscopy and digital radiography.
3	Fluoroscopy: 40-110 Kv; Minimum 7.2 MA @ 110 KV
4	Digital exposures with a minimum tube current of 19 Ma @ 110 kv
5	X-ray tube should be monoblock with active oil circulation
6	The system should operate at full capacity on 220 volts AC, 15amp.
7	The generator should provide digital pulse fluoroscopy with pulse rates of at least 15 frames/second.
8	The system should offer a filtration of 5.5 mm which should include copper filtration for pediatric cases
9	The focal spot size should be 0.6 mm & 1.2 mm dual focal spots.
10	Automatic dose rate control
11	Integrated laser high localizer, radiation-free collimation
12	Multifunction foot switch to control all operating modes and single image storage out of the sterile field.
13	Inbuilt heat management capabilities for long interventional procedures.
15	Metal Artifact reduction/metal correction should be available in fluoroscopy and not as post-processing
C	**Flat Panel Detector System**
1	Flat detector of CsI (Cesium Iodide) with amorphous Silicon doping.
2	Size of detector: min 20 X 20 cm.
3	The pixel size should be 200 microns or less with 1-bit A/D conversion.
4	The resolution of the detector must be 1K x 1K.
5	Image inversion: right to left top to down
6	Provide a last image hold capability that the last image is displayed on the active monitor after the termination of exposure.
7	Equipped with two high-resolution 19" HD LED/TFT medical grade monitors with an image matrix of 1024 x 1024 or more.
8	Vertically and horizontally adjustable monitor for specific needs.
10	Viewing angle of at least 178 degrees with the ergonomic mounting of the monitors on the mobile view station.

Raju Sharma

11	The system should be equipped with a touchscreen control panel. On the patient table side with preview images.
12	The system shall allow the user to change the image orientation on the display screen during a live exposure or using the last image hold. Those functions include image rotation, left-to-right, and top-bottom image reversals.
D	**Digital System & Image Management**
1	Multi-patient database for handling large quantities of images, including dose management reports.
2	Automatically select proper Imaging parameters, kVp, and mA during an image, but also allow the user to override these settings manually.
3	Real-time and automatic brightness and contrast should be provided to optimize the displayed image.
4	The system should save at least 140000 images to the internal hard disk and retrieve stored images later
5	The system should be equipped with a touch-screen control panel on the patient table side with a facility to preview images
6	Two high-resolution 19" HD LED/LCD/TFT monitors with Diagnostic Image quality with an image matrix of 1024 x 1024 or more in the exam room.
7	Provide a real-time post-processing edge enhancement capability to get better image quality according to the density of the tissue. An electronic zoom function, an automatic save function to hard disk, Mosaic Display.
8	It should have a facility to record online fluoroscopy.
9	Should have facility for image and Fluoro sequences retrieval on a CD/DVD/Pen drive and print Images on paper/ firm.
10	The system should have a facility for DICOM connectivity and DICOM ready (HIS compatible, DICOM modality worklist, DICOM send/ receive, DICOM print, DICOM query retrieve). All DICOM functions should be offered and installed when needed at no additional cost.
11	Operating system Windows 10 Pro operating system. Should be the latest version of Windows that the system can support. Any updates/upgrades/patches to the OS and the application should be provided free of cost for the entire period of warranty and CAMC
12	It is the vendor's responsibility to connect the system to the closest network switch in the hospital network and to configure the system with HIS/RIS/PACS
13	Optional item: 3 tray Dry laser Printer to be supplied (at least 500 dpi)
E	**Essential Accessories.**
1	Zero Lead Aprons - 02 nos
2	Thyroid Shield - 02 nos.
3	Sterile covers for C-Arm, X-ray tube, and flat panel detector (disposable):100 for each
4	Lead goggles: 2 nos.
H	**Terms & Conditions:**
1	The company should be ISO 13485 / CDESCO / FDA / European CE certified.
2	During the CMC period, the QA for the unit must be done by the supplier as per AERB requirements.
3	The unit should be approved by AERB.
4	The company should have a proven track record in the Govt. sector.
5	The company is to give an undertaking that the detector will be replaced with the same detector that was quoted during the initial offer for the entire warranty period and the CMC period. No change in detector company is acceptable in case of replacement during the warranty /CMC period

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: MoUs/MoCs/Agreements, which are negotiated between Indian institutions and foreign institutions and universities - reg.

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, Dec 18, 2025 at 11:04 AM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **Director .** <director@aiimspatna.org>
Date: Wed, Jan 29, 2025 at 1:02 PM
Subject: Fwd: MoUs/MoCs/Agreements, which are negotiated between Indian institutions and foreign institutions and universities - reg.
To: medical superitendent <ms@aiimspatna.org>, Dean - AIIMS, Patna <dean@aiimspatna.org>, DDA AIIMS PATNA <dda@aiimspatna.org>

Sd/-
Prof. (Dr.) Saurabh Varshney
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109

---------- Forwarded message ---------
From: **pmssysection iv** <pmssysectioniv@gmail.com>
Date: Wed, Jan 29, 2025 at 11:14 AM
Subject: MoUs/MoCs/Agreements, which are negotiated between Indian institutions and foreign institutions and universities - reg.
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, Executive Director Raebareli <edaiimsrbl@gmail.com>, <rajwanshiarvind@hotmail.com>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, <madhabananda@gmail.com>, <sachimohanty@rediffmail.in>
Cc: Cc: <Dinesh.kumar14@nic.in>, : <Ak.biswas57@nic.in>, Taranjeet Singh <taranjeet.singh@nic.in>, Mr.SankarGarg Mr.SankarGarg <sankar.garg@gov.in>, Amit Batra <amit.batra@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officials of PMSSY-IV Section at - dinesh.kumar14@nic.in; ak.biswas57@nic.in; sankar.garg@gov.in; amit.batra@gov.in

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

OFFICE MEMORANDUM (7).pdf
8306K

E0.4063639/25

No.L-20025/330/2024-IC
Government of India
Ministry of Health and Family Welfare
(International Cooperation Section)

504-D, Nirman Bhawan, New Delhi
Dated the 21st January, 2025

OFFICE MEMORANDUM

Subject: MoUs/MoCs/Agreements, which are negotiated between Indian institutions and foreign institutions and universities - reg.

It has been noted that several hospitals/research institutions and autonomous bodies within this Ministry are entering into Agreements/MoUs with foreign countries/institutions on varying subjects, including joint research and collaborations with variations in procedures being followed. Concerns have also been raised regarding the sharing of data and intellectual property rights.

2. To streamline the process and provide clarity to the process, the following general guidelines are being circulated to all divisions to be noted while entering into any Agreement/MoU/MoC/JDI etc. with any foreign government, research institution or other entity.

a) All institutions may refer to the Standard Operating Procedure issued by the Ministry of External Affairs vide Letter No.312/AS(MD)/17 dated 2nd April, 2018, read with Letter No.05/Monitoring Cell/17 dated 29th August, 2017 (copies enclosed) for general guidance on entering into MoU/JDI/MoCs with foreign governments/research institutions.

b) The level of approval to be taken may be identified by the institution in consultation with their programme division, if need be. In the case of Autonomous Bodies, the approval from the Governing Body is imperative before proceeding to approve such agreements.

c) All organisations are to exercise caution regarding the safety, security and integrity of the research, including intellectual properties. It is imperative that due regard may be paid to ensure that research exchange under such MoUs, Agreements etc. is balanced, mutually beneficial and it does not result in the alienation of intellectual property. Therefore, consultation with Department for Promotion of Industry and Internal Trade (DPIIT) is mandatory in all cases.

d) All proposals to be undertaken involving foreign-funded/collaborative research proposals on biological sciences are to be forwarded for mandatory approval through Biological Research Regulatory Approval Portal (BioRRAP) (https://biorrap.gov.in) under Department of Biotechnology. This portal provides a single route to direct the applicant to regulatory agencies providing requisite approval relevant to the biological research.

e) All such agreements/MoUs etc. must be legally vetted before submission for approvals.
f) A copy of the MoU may be forwarded to the International Cooperation division for record.

3. It is also requested keep the IC Division in the loop while negotiating the bilateral instruments with foreign countries, agencies etc.

4. This issues with the approval of Secretary (HFW).

Encl.: As above.

Digitally signed by DASARI RAMESH BABU
Date: 21-01-2025 15:14:40

(D. Ramesh Babu)
Under secretary to the Govt. of India
Tel: 011-23062796
Email: dramesh.babu@nic.in

1. All Additional Secretaries & equivalent / Joint Secretaries & equivalent of Ministry of Health & Family Welfare.

2. Heads of all Attached / Subordinate Organizations / Statutory Bodies / Autonomous Organizations of Ministry of Health & Family Welfare.

A. Gitesh Sarma
Additional Secretary(MD)

No. [illegible]/AS(MD)/17 Dated [illegible] 2018

Subject: Revision of Standard Operating Procedures (SOPs) with respect to MoUs/ Agreements with foreign countries.

Dear Secretary,

Please refer to this Ministry's DO No. 05/ Monitoring Cell/17 dated 29.8.2017 on the aforementioned subject forwarding the revised SOPs to various Ministries, which provide guidance with regard to entering into MoUs/ Agreements with foreign countries.

2. The SOPs circulated earlier have been partially modified under para 'G' of the SOPs to provide for exemption from uploading those which are of a classified nature. A copy of the updated SOPs is enclosed. This issues with the approval of Foreign Secretary.

Yours Sincerely,

(A Gitesh Sarma)

Secretaries of all Ministries as per list

Ministry of External Affairs, Jawahar Lal Nehru Bhawan, Delhi -110011
Tel. +91-11-49015407; E-mail: aspol@mea.gov.in

File No. [illegible] (Computer No. [illegible])
Generated from eOffice by [illegible]

Guidelines/SoP on the conclusion of International Treaties in India

CONTENTS:

Particulars	Page Number
A. International Practice	2
• Different Nomenclatures used by States in their practice	3
B. Indian Practice	5
C. Role of MEA (L & T Division)	5
D. Treaty making formalities	5
(i) Drafting and Negotiation	5
(ii) Approvals	6
(iii) Full Powers	8
(iv) Ratification	8
(v) Accession	9
(vi) Credentials	10
(vii) Amendment of a Treaty	10
(viii) Review of Treaties	10
E. Guidelines/SoP concerning the conclusion of Twinning Agreements with the Provincial Governments of Foreign Countries	10
F. Guidelines/SoP concerning the Twinning Arrangement between the Cities	12
G. Indian Treaty Database Section (Maintained by the Legal and Treaties Division)	12
ANNEX – I Checklist - for the purpose of concluding bilateral Treaties	13
ANNEX – II Structure/Format of an Agreement (MoU)	15

****

File No. L-20025/330/2024-IC (Computer No. 8311810)
Generated from eOffice by NIKHIL BANSAL, ASO(NB)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 22/01/2025 02:48 pm

The guidelines/SoP and practice concerning negotiation and conclusion of international treaties and related aspects thereto are set out below:

A. International Practice:

Under international law, the law and practices pertaining to treaties is governed by the Vienna Convention on the Law of Treaties, 1969. Although, India is not a Party to the Convention, it follows its provisions in practice. The Convention codifies the law, practice including norms concerning the international treaty making. The Vienna Convention refers to **'treaty'** in its generic sense and defines as "an international agreement concluded between States in written form and governed by international law, whether embodied in a single instrument or in two or more related instruments and whatever its particular designation".

Thus, the term 'treaty' covers all forms of international instruments, namely, treaty, convention, agreement, memorandum of understanding, , protocol, etc., irrespective of nomenclature, all negotiated and concluded international instruments create legal rights and obligations between the parties.

The parties to a treaty may agree for its entry into force either on the date of signature, or may make entry into force subject to ratification. In the former scenario, the treaty will become effective immediately on signing. Where, however, entry into force of a treaty is subject to ratification, signing would only reflect the intent of the country concerned to be bound to its provisions, and will have the binding effect only on ratification.

The "treaties" assume a variety of form and style, but they are all governed by the law of treaties, which is part of customary international law. Different nomenclatures used in the international relations are: Agreement, Convention, Protocol, Memorandum of Understanding, Memorandum of Cooperation, Memorandum of Association, Charter, Covenant, Pact, Statute. There are less formal agreements sometimes through "exchange of notes" "letter of intents", or "exchange of letters."

File No. L-20025/330/2024-IC (Computer No. 8311810)
Generated from eOffice by NIKHIL BANSAL, ASO(NB)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 22/01/2025 02:48 pm

Different Nomenclatures used by States in their practice:

- **Treaty:** Used for formal agreements between States, subject matter and provisions of which are governed by international law. A 'treaty' is a formally concluded and ratified agreement between States. The term is used generically to refer to instruments binding at international law, concluded between international entities (States or organizations). Under the Vienna Conventions on the Law of Treaties, a treaty must be (1) a binding instrument, which means that the contracting parties intended to create legal rights and duties; (2) concluded by states or international organizations with treaty-making power; (3) governed by international law and (4) in writing[1]. Treaties may be bilateral (two parties) or multilateral (between several parties) and are usually binding only on the parties thereto.

- **Convention:** Usually used for multilateral agreements. This generic term is synonymous with that of "treaty". Conventions are normally open for participation by the international community as a whole, or by a large number of States. Usually the instruments negotiated under the auspices of an international organization are entitled conventions[2].

- **Agreement:** Formal and legally binding arrangements with a defined scope and fewer parties. Agreements are the instrument by which states and other subjects of international law, such as certain international organizations, regulate matters of concern to them. Agreements are more often used in the bilateral contexts. Again, the "agreement" is also synonymous of "treaty".

- **Protocol:** Usually an ancillary agreement to the existing instrument.

- **Declaration:** The term 'declaration' is normally used for bilateral or multilateral instruments which by nature are declaratory and not legally binding. For instance, human rights declaration.

- **Memorandum of Understanding (MoU):** A less formal agreement, usually of an administrative or technical in nature. MoU is used where the subject matter is not essentially governed by the international law. MoUs are preferred where the

[1] UNICEF Document on the Convention on the Rights of the Child
[2] https://www.britannica.com/topic/international-agreement

matter being essentially technical or administrative in nature which may change frequently according to suitability of the Parties. For e.g. in the fields of education, technology, cultural cooperation, sports, youth affairs, etc.

As per the practice of many of the countries around the world (for e.g. the US), the key difference between MoUs and treaties is whether or not there is an intention to create legally binding obligations. However, Indian practice does not fully subscribe to this idea wherein the nature of the instrument is determined based on its contents and not on the basis of its title.

- **Memorandum of Cooperation (MoC):** A less formal agreement, usually of an administrative or technical nature of limited duration. MoCs could be concluded under the umbrella of a certain framework agreement. It is synonymous of MoU.

- **Memorandum of Association (MoA):** Akin to MoU and MoC, these are less formal arrangements designed for starting cooperative activities and exchanges. MoAs could be concluded under the umbrella of certain framework agreement.

- **Letter of Intent/Statement of Intent:** The letter of intent (LoI) is a non-binding statement that acknowledges parties' intent to explore the possibility of collaboration and cooperation in the relevant areas contained therein. Letters of intent are appropriate when a new project/undertaking is being initiated, and the specific areas of formal cooperation between parties are yet to be identified and negotiated. The letter of intent can serve as a gesture and the willingness to discuss the possibilities and opportunities to establish cooperation in certain areas. On the identification of specific areas and reaching the stage of preparedness and maturity, the parties may negotiate and conclude formal treaty

- **Exchange of Notes/Letters:** It is a method of concluding an agreement in situations where due to time constraint or emergency, States do not have enough time to negotiate a formal agreement. This method may also be used for amending/terminating an existing instrument through diplomatic channel.

Notes may also be exchanged to extend the validity of a treaty. The exchange of notes and correspondences related thereto is conducted through the

File No. L-20025/330/2024-IC (Computer No. 8311810)
Generated from eOffice by NIKHIL BANSAL, ASO(NB)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 22/01/2025 02:48 pm

diplomatic channels.

Therefore, the choice of the nomenclature depends upon the negotiating States. The determination of status of an international instrument as an international treaty in terms of Vienna Convention on Law of Treaties depends on the contents thereof and the factor whether or not that instrument is governed by international law.

B. Indian Practice:

According to the Indian Constitutional scheme, making of international treaties is an executive act. A Treaty is concluded with the approval of the Union Cabinet. It is not placed before the Parliament for discussion and approval. However, where the performance of treaty obligations entail alteration of the existing domestic law or requires new enactment, it would accordingly require legislative action.

C. Role of MEA (L & T Division):

The Legal and Treaties Division of MEA renders legal opinion on all international law issues to the Government as a whole. It scrutinizes international instruments for consistency with international law and with India's international rights and obligations. The Division forms part of Indian delegations, in the capacity as legal advisers, in international conferences, and in bilateral negotiations locally and abroad. The Division participates in the drafting of Indian legislation giving effect to the provisions of a treaty in India including amendments thereof, when required, for implementing the treaty obligations. On conclusion, treaties are forwarded to the Legal and Treaties Division for depository functions and safekeeping.

D. Treaty making formalities:

(i) Drafting and Negotiation:

The Ministry of External Affairs is overall in-charge of international treaty making activities. The administrative Ministry is the nodal agency for preparation of drafts, consultations and negotiations.

Multilateral treaties are mostly negotiated in international conferences. In

File No. L-20025/330/2024-IC (Computer No. 8311810)
Generated from eOffice by NIKHIL BANSAL, ASO(NB)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 22/01/2025 02:48 pm

the case of bilateral treaties, concerned administrative Ministry, on preparation of draft text of the treaty, in consultation with other stake holders, submits the same with the approval of the Minister concerned to the Ministry of External Affairs (Legal and Treaties Division) for vetting before it is sent to the other country for consideration, through diplomatic channels.

To the extent possible, modern means of communication including emails, video conferencing, teleconference should be used by the stakeholders to negotiate bilateral treaties except, security related matters.

(ii) Approvals:

After the text of the Treaty has been negotiated and finalized, the administrative Ministry processes for necessary approvals of the Minister concerned and thereafter the External Affairs Minister's approval is obtained. The administrative ministry then moves Cabinet Note for its approval.

According to the Second Schedule to the Government of India (Transaction of Business) Rules, 1961, the approval of the Cabinet is imperative for all treaties (which include conventions, agreements, MoUs, MoCs, MoAs & protocols etc.,) to be signed with any foreign agency/country[3]. These instructions are also applicable to all subordinate/attached offices including Statutory bodies and authorities of Ministries/Departments and the various Commissions under the Constitution[4], except in the following cases:

(a). Cultural Agreements and Agreements on Science and Technology not impacting the national security or our relations with other countries which are d*uly approved by the Minister-in-Charge of the Department* concerned and the *Minister of External Affairs and where requisite inter-Ministerial consultations in terms of rule 4 have been carried out* may only be circulated to the Cabinet for information;

[3] Refer para 2(ii) of the Cabinet Secretariat's O.M. No.1/48/6/2015-Cab, dated 3 June 2015; O.M. No. 1/48/6/2015-Cab, dated 24 April 2015; O.M. No. 1/50/3/2014-Cab., dated 9 February 2014.
[4] Refer para 2(iii) of the Cabinet Secretariat's O.M. No.1/48/6/2015-Cab, dated 3 June 2015;

File No. L-20025/330/2024-IC (Computer No. 8311810)
Generated from eOffice by NIKHIL BANSAL, ASO(NB)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 22/01/2025 02:48 pm

(b). Such *foreign Aid Agreements and Commercial Agreements*, which are duly *approved by the Minister-in-charge of the concerned Department* and as are within the broad frame-work already approved by the Cabinet need not be formally placed before the Cabinet.

In case of any doubt as to whether approval of Cabinet is required for concluding a particular agreement/MoU, the matter may be referred by the Administrative Ministry to the Cabinet Secretariat for a decision. Proposal for obtaining the Cabinet approval should be sent to the Cabinet Secretariat well in advance obviating the need for rushing such proposals at the last moment[5]. However, the Ministries/Departments may submit the proposal under Rule 12 of the Government of India (Transaction of Business) Rules, 1961 **only** if there is an extreme urgency or unforeseen contingency. Cabinet Notes seeking approval for signing of MoUs are to be prepared sufficiently in advance of the proposed visit so as to preclude the need to seek approval under Rule 12[6]. If MoUs requiring prior Approval of the Cabinet are signed after obtaining approval under Rule 12, they are required to be submitted for *ex post facto* approval of the Cabinet or for information as the case may be, within **one month** of the signing of such MoU. In case of any delay, the Note should detail the specific reason(s) and justification(s) in submitting the Note before the Cabinet after the prescribed time period[7].

The Ministries/Departments using the title of the instrument as MoU, it must provide the rationale for the same while sending to the Cabinet. Ministries/Departments should also enclose a list and status of existing MoUs while seeking approval of a new MoU[8].

After obtaining the necessary approvals, as indicated above, the text of treaty/agreement may formally be signed and concluded with foreign governments. For the purpose of signing, the concerned administrative Ministry, in consultation with the MEA, designates a person to sign the treaty representing the Government of India.

---

[5] Cabinet Secretary's D.O. No. 1/13/4/2017-Cab., dated 22 November 2007; D.O. No.1/3/2/2012-Cab., dated 23 November 2012.
[6] Cabinet Secretary's D.O. No. 1/48/6/2015-Cab., dated 24 June 2015
[7] Cabinet Secretary's D.O. No. 1/48/6/2015-Cab., dated 14 August 2015
[8] Cabinet Secretariat's O.M. No. 1/48/6/2015-Cab., dated 3 June 2015; Cabinet Secretariat's O.M. No. 1/50/3/2014-Cab., dated 9 February 2015.

File No. L-20025/330/2024-IC (Computer No. 8311810)
Generated from eOffice by NIKHIL BANSAL, ASO(NB)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 22/01/2025 02:48 pm

(iii) Full Powers:

The person designated for signing the treaty would require Full Powers from the President of India authorizing him to sign. The Concerned administrative Ministry provides the name, title, position, etc. of the person designated to be named in the Instrument of Full Powers, along with the finalized text of the treaty, Cabinet Note and the Cabinet approval to the Legal and Treaties Division, which prepares and processes the Instrument of Full Powers for favour of the signature of the President.

It may however be noted that the Head of the State, Head of Government and Minister for Foreign Affairs, do not require Full Powers to sign or authenticate a treaty, by virtue of their office and functions. Thus, based on the international law and practice, the President, Prime Minister and the External Affairs Minister of India do not require Full Powers.

Ambassadors or High Commissioners may initial treaties with the country to which they are accredited. They would however require Full Powers if designated to sign the treaty formally.

Full Powers are not required when a treaty is signed in the presence of the President or the Prime Minister of India.

(iv) Ratification:

Where a treaty does not provide for its entry into force upon its signature only, and makes it subject to ratification, the treaty requires ratification. Multilateral Treaties are, however, always subject to ratification. The treaty is ratified by obtaining the Instrument of Ratification under the signature and seal of the President of India.

In order to ensure that India is in a position to efficiently discharge all obligations emanating from the treaties/agreements, ratification/accession should be undertaken only after the relevant domestic laws have been amended, or the enabling legislation has been enacted in cases where there are no domestic laws on the subject. Therefore, proposal for entering into such treaties/agreements should specifically state that such ratification or accession will be made only **after**

File No. L-20025/330/2024-IC (Computer No. 8311810)
Generated from eOffice by NIKHIL BANSAL, ASO(NB)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 22/01/2025 02.48 pm

amending the relevant domestic laws, or enacting appropriate legislations[9].

The Concerned administrative Ministry submits the Cabinet Note, Cabinet approval and three clean copies of the signed treaty in Hindi (where signed in Hindi) and in English languages. The instrument of ratification is prepared by the Legal and Treaties Division of MEA and processed for favour of signature of the President.

In case of a bilateral treaty, it becomes effective on the exchange of instruments of ratification or through notification, as the case may be, which will be effected through diplomatic channels.

In case of a multilateral treaty, the instrument of ratification is to be deposited with the depository to the treaty. The States may agree to a specific number of ratifications required for its entry into force.

(v) Accession:

Accession is the procedure for becoming a party to a treaty where a country has not signed the treaty during the period it was open for signature. In such a situation, a country accedes to the treaty without having signed it. Most of the multilateral treaties provide for accession, through which States may become Parties to such treaty.

The Concerned administrative Ministry is required to submit the Cabinet Note, Cabinet approval and three clean copies of the treaty to L&T Division. The instrument of accession is prepared by the Legal and Treaties Division of MEA and processed for favour of signature of the President. It is then deposited with the depository of the Treaty.

(vi) Credentials:

Credentials confer the authority to participate in negotiations as representatives of the Government of India, and to initial the treaty at the conclusion of negotiations. The purpose of initialing is to confirm the status of the text of the treaty negotiated. The credentials where required, are obtained by the

[9] Cabinet Secretariat's O.M. No. 1/13/2/2010-Cab., dated 23 August 2011

File No. L-20025/330/2024-IC (Computer No. 8311810)
Generated from eOffice by NIKHIL BANSAL, ASO(NB)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 22/01/2025 02:48 pm

concerned Territorial Division of MEA.

(vii) Amendment of a Treaty:

Normally, treaties contain provisions in their final clauses stipulating procedure for their amendment. The parties may agree for amendment of the treaty at any time by mutual written consent of the parties. A state party may, at any time, propose an amendment, which, on negotiations, may be approved or rejected in whole or in part by the parties. The parties may agree for the entry into force of an amendment either through the same procedure as applicable for the entry into force of the treaty or a different one.

(viii). Review of Treaties:

Most of the bilateral Agreements/MoUs contain a clause for the periodical review of the activities undertaken under the Agreements/MoU. Besides, the Concerned Ministries shall review their treaties from time to time and shall send a report at the end of each year to the concerned Territorial Division of MEA apprising about the implementation activities undertaken, and the status of the treaty i.e. whether its validity is continuing or has expired. If expired whether it is to be renewed or there is no necessity of renewal.

E. Guidelines/SoP concerning the conclusion of Twinning Agreements with the Provincial Governments of Foreign Countries:

Ministry of External Affairs has considered the emerging trend of State Governments/agencies in entering into Agreements with the provincial Governments of other Countries for promoting/enhancing cooperation in investments, industry, commerce, culture, health, tourism and other areas and is of the view that such proposals should be considered on a case-by-case basis by the concerned Administrative Ministry, taking into account the nature, scope and overall usefulness of the understanding being entered into.

The Policy of twinning may include the following elements:

i) Twinning may be considered where they could lead to expansion of investment, trade, technological, culture, tourism, educational and other cooperation to the benefit of India.

File No. L-20025/330/2024-IC (Computer No. 8311810)
Generated from eOffice by NIKHIL BANSAL, ASO(NB)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 22/01/2025 02:48 pm

ii) Proposals for twinning of bordering States with their counterparts in neighboring countries involving issues relating to policies and security will normally not be agreed to.

iii) A broad plan of cooperation with details of cooperative activities will be submitted by the State interested in entering into twinning arrangements with the province of a foreign State along with the financial resources available for carrying out such activities. iv) The process for completing agreements between States/Provinces need to be carefully examined by the concerned Ministry with other stakeholders before sending for MEA's approval, including vetting by the MEA (Legal and Treaties Division).

v) The Ministry of External Affairs must be kept informed of all treaties/Agreements/MoUs related actions, such as signature, and entry into force, action plan, and review status. The copy of all concluded Agreements/MoUs should be sent to the Ministry of External Affairs (L&T Division) for information and record purpose.

vi) There should be a review of the twinning arrangements annually. The Concerned State Government will send a report at the end of each year to the concerned Territorial Division of MEA and concerned administrative Ministry about the implementation of arrangements and their status i.e. whether its validity is continuing or has expired. If expired whether renewed or there was no necessity of renewal. In case any activity has negative or adverse implications on our national interest or bilateral relations, it shall be immediately discontinued. Twinning may be allowed only with a limited number of foreign provinces.

vii) These instructions are applicable to all subordinate/attached offices including statutory bodies and authorities of Ministries/Departments of the State Government and the various Commissions under its authority.

F. Guidelines/SoP concerning the Twinning Arrangement between the Cities:

Ministry of Urban Development (MoUD), Government of India is the nodal Ministry at the central level for the Scheme Twinning Arrangements between the

Indian Cities and that of foreign countries.

In case of proposal for arrangement with a foreign city, the State Government concerned should follow the guidelines issued by the MoUD. After it is agreed to twin a foreign city with an Indian city, an agreement may be reached on specific objectives of twinning within the broad framework of objectivities.

After scrutiny of the proposal submitted by the State Government, the MoUD shall seek the concurrence from Ministry of External Affairs (political and legal angle) before finalizing the said arrangement.

G. Indian Treaty Database Section (Legal and Treaties Division):

The Treaty Section in the Office of the Legal and Treaties Division is the official custodian of all international treaties to which India is a party. Other Administrative Ministries deposit all original treaties and certified copies of multilateral treaties as well as any necessary communiqué/documents concerning the status and implementation of international treaties with the MEA (Legal and Treaties Division) for custodial purposes. As soon as treaties are signed, the concerned Ministries/Departments or Divisions of the MEA are required to send their soft copies (both in Hindi and English), which are not classified/confidential in nature[10], to the Legal and Treaties Division for the purpose of uploading them into the Indian Treaty Database at MEA website **(www.mea.gov.in/Treaty.htm)**.

[10] As per the Government of India policy, classified/confidential treaties are exempted from posting/uploading on the Indian Treaty database. *Ref*: Cabinet Secretariat's Communiqué I.D.No. 141/1/11/2016-TS, dated 03-01-2018).

ANNEX- I

Checklist to be followed for the purpose of concluding bilateral Treaties:

1. The Ministry of External Affairs & concerned Administrative Ministry hold consultation about the desirability of a Treaty with a particular country;
2. The Administrative Ministry moves the proposal/Draft through MEA to the country concerned for consideration;
3. Administrative Ministry, in consultation with stakeholders, prepares a draft;
4. The Administrative Ministry make sure that the text of the treaty is seen and vetted by the MEA (Legal and Treaties Division) before proposing to the foreign country concerned for consideration;
5. The composition of the Indian delegation for negotiating treaties should include representatives of MEA to ensure proper advice on international legal issues and policy;
6. In case of bilateral negotiations, all correspondence regarding the scheduling of negotiations, composition of delegations, dates of signing, exchange of ratification instruments etc. should be forwarded through the Ministry of External Affairs;
7. Views/opinion on the treaty's consistency with **domestic law** must be obtained from the Department of Legal Affairs, Ministry of Law and Justice;
8. Cabinet Notes proposing for seeking Cabinet approval for signing and ratification/accession of treaties must be sent to the Ministry of External Affairs for approval/concurrence from the political and legal angles;
9. Full Powers from the President of India authorizing the person named to sign a treaty on behalf of the Government of India should be obtained;
10. Requests for obtaining Instruments of Full Powers, Ratification and Accession must be sent to the MEA along with the required documentation/approvals;
11. Requests for credentials for participation in international conferences should be obtained through the UNES Division of the Ministry of External Affairs;

File No. L-20025/330/2024-IC (Computer No. 8311810)
Generated from eOffice by NIKHIL BANSAL, ASO(NB)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 22/01/2025 02:48 pm

12. The Ministry of External Affairs must be kept informed of all treaty actions, such as signature, ratification and entry into force. The original instrument of all treaties should be sent to the Ministry of External Affairs (L&T Division) which is the custodian of all treaties of Govt. of India for record purpose.

[Should any clarification be required on the above guidelines, it could be sought from **Joint Secretary (L&T), Ministry of External Affairs** [Tel: 49015269; Fax: 49016643; **email**: jslegal@mea.gov.in]

****

ANNEX- II

STRUCTURE/FORMAT OF AN AGREEMENT (MOU):

Drafting of Treaties:

As all elements of international agreements need to be agreed by the respective parties. The drafting style will also depend on the agreement between the parties. The guidelines on drafting are therefore indicative although not necessarily always attainable.

An Agreement/MoU needs to be in the below format:

A. Title & Parties

B. Preamble/Recitals

I. **Article - I: Definitions**

II. **Article - II: Objectives**

III. **Article - III: Areas of Cooperation**

IV. **Article - IV: Forms of Cooperation**

V. **Article - V: Central Authority**

VI. **Article - VI: Implementation & Joint Working Group**

VII. **Article - VII: Financial Arrangement**

VIII. **Article - VIII: Protection of Intellectual Property Rights**

IX. **Article - IX: Protection of Confidential Information**

X. **Article - X: Revision & Amendment**

XI. **Article - XI: Settlement of Disputes**

XII. **Article - XII:: Entry into Force, Duration, Renewal & Termination**

C. Concluding Paragraph

D. Signature Clause

The Parties:

File No. L-20025/330/2024-IC (Computer No. 8311810)
Generated from eOffice by NIKHIL BANSAL, ASO(NB)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 22/01/2025 02:48 pm

Treaties are concluded between governments/departments. The Indian side is cited as *"the Government of the Republic of India"*.

Sequencing of articles:

If an article on "Definitions" is required, this should be placed at the very beginning of the Treaty just after the Preamble. Definitions should be listed in alphabetical order.

If an article on the "Objective" or "Purpose" is included, it should be included after the article on Definitions. Substantive clauses follow the definitions. Standard articles on Settlement of Disputes, Amendment and the final clauses on Entry into Force and Duration and Termination follow the text of the Treaty.

Preamble/Recitals:

An international Treaty usually has a preamble that is not intended to constitute substantive provisions or create legal obligations. However, preamble works as a window through which the substance of trety provisions and intent of negotiating parties is peeped into. The contents and the size of preamble depends on subject and nature of the treaty.

Preamble sets out the background and context of the Treaty and is used as an aid to the interpretation of the Treaty.

Example:

RECALLING that an Agreement was entered into on 19 September 1969 between the Government of the Republic of India and the Government of the _____ concerning the establishment and operation of a _____ scheme, for the _____ (purpose) for use within the territories of India and other countries;

RECOGNISING that conditions have changed considerably since the conclusion of the said Agreement, which consequently no longer reflects the realities of the situation in the region;

DESIRING THEREFORE to enter into a bilateral Agreement which will take account of the changed conditions prevailing in the region;

HAVE AGREED AS FOLLOWS:

Or

"WHEREAS the Government of the Republic of India and the Government of the _____ (hereinafter individually referred to as the "Party or Contracting State or Participant" and jointly referred to as the "Parties or Contracting States or Participants"); are desirous to consolidate and strengthen their friendly ties and reciprocal understanding; and

WHEREAS the Parties are conscious of the desirability of promoting, to the greatest possible extent the mutual knowledge, experience and understanding of their respective human and developmental needs in the field of _____, by means of friendly cooperation between them;

Have reached the following understanding:

Headings and numbering:

It is always helpful if headings/subtitles are provided for each Article.

The substantive provisions are divided into Articles, Sub-Articles, Paragraphs and Sub-Paragraphs. Articles are numbered either in Arabic or capital Roman numbers.

Sub-articles are numbered in Arabic numbers, paragraphs in alphabetic letters and sub-paragraphs in small Roman numbers. Capital letters are used and the Article and Subtitle are centered. e.g.

ARTICLE 4

or

ARTICLE IV

AREAS OF COOPERATION

Areas of Cooperation

Considering the requirement, the Parties may list out the areas of cooperation.

File No. L-20025/330/2024-IC (Computer No. 8311810)
Generated from eOffice by NIKHIL BANSAL, ASO(NB)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 22/01/2025 02:48 pm

Each Party will endeavor to take necessary steps to encourage and promote cooperation in the following areas and/of forms:

a.

b.

c.

Forms of Cooperation

In which forms the cooperative activities are proposed to be carried out can be listed under this heading.

Specific activities in the areas of cooperation listed in Article I may include cooperation in Research and development, Training, Visit of delegates and experts etc.

In case MoU contemplates exchange of resource persons, experts or students as a form of cooperation, eligibility/process for selection of such participants as well as the frequency of such programmes should be included in the MoU.

Action Plan, Objectives & Deliverables

The action plan is a dynamic strategy for meeting the requirements of the MOU drawn by the Administrative Ministry. Action plan contains the list of deliverables, scope and areas of cooperation contemplated under the framework of an MoU. Therefore, MoUs should spell out specific objectives to be achieved by comprehending all the activities to be included in the MoU. Scope and areas of cooperation should be clearly mentioned.

These activities are to be listed item-wise based upon the object to be achieved under the MoU and the intention of the Parties thereto.

Central Authorities

The Agreement/MoU should identify the Central Authorities respectively, who are the nodal points for contacts to each of the Parties under the

File No. L-20025/330/2024-IC (Computer No. 8311810)
Generated from eOffice by NIKHIL BANSAL, ASO(NB)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 22/01/2025 02:48 pm

Agreement/MoU. The Central Authority is responsible for implementation of the schemes of the treaty including receiving, sending, examining the requests.

The Parties shall designate the following authorities as Central Authorities to implement the provisions of the Agreement/MoU.

Implementation/Review

Implementation of the provisions of an Agreement/MoU vests with the mechanism created under the MoU. It is preferable for the Administrative Ministries to have a periodic review of the activities undertaken under the MoU. Therefore, an institutional set up, within the framework of an Agreement/MoU may be set-up.

"Within the framework of this Agreement/MoU, in order to exchange views and draw a road map for enhancing cooperation, both sides may constitute a Joint Working Group (JWG). JWG is composed of equal number of the representatives from each side. Such a Joint Working Group may conduct periodical meetings and reviews, preferably bi-annually, in the respective countries alternately".

or

"The Parties shall hold working level meeting in order to implement the purpose of the Agreement/MoU effectively, and the details of such meetings will be decided by the Working level meeting".

Financial Arrangement

Financial modalities to carryout the activities mentioned in the MoU need to be set out under this paragraph. This may include joint sharing of expenses; travel expenses arrangement and so on.

Protection of Intellectual Property Rights

If any research activity or productive activities giving rise to intellectual property rights, the ownership and utilization of the same may be provided here. This clause needs to be cleared by the Department of Industrial Policy & Promotion (DIPP)

Protection of Confidential Information

File No. L-20025/330/2024-IC (Computer No. 8311810)
Generated from eOffice by NIKHIL BANSAL, ASO(NB)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 22/01/2025 02:48 pm

If any confidential information, trade secrets are exchanged, a clause to protect them from disclosure may be included.

All information and documents to be exchanged pursuant of the MoU will be kept confidential by the Parties and will be used subject to such terms as each Party may specify. The Parties will not share such information with third Parties or use the information for purposes other than that specified, without the prior written consent of the other Party.

Settlement of Disputes

If any difference arises between the Parties while carrying out the activities under the MoU, it shall never be referred to international adjudication. Unless it is in commercial in nature, arbitration should also be avoided.

"Any dispute between the Parties arising out of the interpretation or implementation of this Agreement shall be settled amicably through consultation or negotiation between the Parties to the dispute."

Amendment

An Agreement/MoU usually would have a provision for amendment like:

"This Agreement may be amended at any time by mutual written consent of the Parties through an Exchange of Notes between the Parties through the diplomatic channel."

Entry into force

"This Agreement shall enter into force on the date of its signature thereof by the Parties."

Or

This Agreement shall be subject to ratification.

Or

This Agreement shall come into force after the completion of the internal legal procedures necessary for the entry into force of the Agreement.

Or

"The Parties shall notify each other in writing when their respective constitutional requirements for entry into force of this Agreement have been fulfilled. This Agreement shall enter into force on the date of the last written notification."

The situations where the Agreement/MoU is not entering into force on signature, and is subject to ratification or completion of constitutional legal procedure etc., would require ratification.

It frequently happens that the other party will require an entry into force clause that requires notification of the completion of the constitutional procedures. This is acceptable. However, the Administrative Ministry should note that the selection of this wording would require an additional administrative step, namely that a Diplomatic Note must be sent. In these cases, the concerned administrative ministry should request the relevant Territorial Division of the Ministry of External Affairs send such a Note.

Where ratification or accession is to be expressively provided for, the correct format must be used in consultation with Legal and Treaties Division.

Duration and Termination

"This Agreement shall remain in force for a period of ..... years. Thereafter, it may be renewed automatically for further successive periods of ..... years at a time"

or

"The Agreement shall continue for a term of three years. Thereafter, it will be renewed for further periods by mutual written consent of the Parties" unless terminated by either Party by giving ..... months written notice in advance to the other Party of its intention to terminate this Agreement through diplomatic channels.

A Party terminating this Agreement shall remain bound to contractual relationships to which it is a party and to its obligations there under, until they are fulfilled.

Or

"This Agreement shall enter into force on the date of signature and remain in force for an indefinite period unless terminated by either Party giving ..... months written notice in advance of its intention to terminate the Agreement through the diplomatic channel.

"Termination of this Agreement shall not affect any programmes undertaken prior to the termination of this Agreement, unless otherwise agreed upon by the Parties."

Or

"The termination of this Agreement shall not affect the completion of any unfulfilled obligation at the moment of its termination, unless otherwise agreed by the Parties."

Renewal Clause:

Renewal clause is to be included based on the requirement of the Administrative Ministry and the wish of the Indian counterparts, keeping in mind the utility and diplomatic relationships. Renewal could be either (i) for a specific period or (ii) for an indefinite duration.

It may be suggested not to have automatic renewal clauses resulting in the indefinite application of the provisions of an Agreement unless it is required from the point view of functional requirement or diplomatic sensitivity. If at all renewal clause is required, it is suggested to be term specific.

"After the initial term, this Agreement/ MoU may be renewed for a further term of.... years".

Or

"This Agreement/ MoU may be renewed for further term(s) as agreed by the Parties in writing".

Or

"After the initial term, the Agreement/ MoUshall be automatically renewed for an equal term until it is terminated by either of the Parties".

Concluding and Signature Clauses

"IN WITNESS WHEREOF the undersigned, being duly authorized by their respective Governments, have signed this Treaty

Done at _____ on _____ day of _____ 20-- in two originals, each in the Hindi, _____ and the English languages, all texts being equally authentic. In case of divergence in interpretation, the English text shall prevail.

Or

Signed/Done at_____ on _____ day of _____ 20-- in two originals in the English language.

FOR THE GOVERNMENT OF THE REPUBLIC OF INDIA

FOR THE GOVERNMENT OF THE _____

Name:

Designation:

Name:

Designation:

****

File No. L-20025/330/2024-IC (Computer No. 8311810)
Generated from eOffice by NIKHIL BANSAL, ASO(NB)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 22/01/2025 02:48 pm

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Subject: Adherence to Rule 20 of the CCS (Conduct) Rules, 1964 by officers/officials of New AIIMS - reg.

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, Dec 18, 2025 at 11:01 AM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **pmssysection iv** <pmssysectioniv@gmail.com>
Date: Wed, Jan 29, 2025 at 9:52 AM
Subject: Subject: Adherence to Rule 20 of the CCS (Conduct) Rules, 1964 by officers/officials of New AIIMS - reg.
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, Executive Director Raebareli <edaiimsrbl@gmail.com>, <rajwanshiarvind@hotmail.com>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, <madhabananda@gmail.com>, <sachimohanty@rediffmail.in>
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, <DDA@aiimsrbl.edu.in>, Dr. PRADIP KUMAR <kpradip10@gmail.com>, <dda@aiimskalyani.edu.in>, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, Rajeev Sen Roy <rajeevsenroy30@gmail.com>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, <dda@aiimsbilaspur.edu.in>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, <sanjaygarg0204@yahoo.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, Administrative Officer <ao.aiimsmadurai@gmail.com>, T Ngamlien <t.ngamlien@icg.gov.in>, Mukesh Kumar <mac.prasad@gmail.com>, <ddaaiimsawantipora1@gmail.com>, Dy Director Administration AIIMS, Raebareli <ddaaiimsrbl@gmail.com>, Cc: <Dinesh.kumar14@nic.in>, : <Ak.biswas57@nic.in>, Taranjeet Singh <taranjeet.singh@nic.in>, Suprava Poddar <sup15.81997@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officials of PMSSY-IV Section at - dinesh.kumar14@nic.in; ak.biswas57@nic.in; taranjeet.singh@nic.in; ; sup15.81997@gov.in;

116

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

2 attachments

Letter (72).pdf
103K

Encl- 28.01.2025.pdf
267K

No. V-28021/44/2024-PMSSY-IV
Government of India
Ministry of Health and Family Welfare
(PMSSY - IV Section)
***

Room No:745A, Nirman Bhawan, New Delhi
Dated 28th January, 2025

To

Executive Directors, All New AIIMS

Subject: Subject: Adherence to Rule 20 of the CCS (Conduct) Rules, 1964 by officers/officials of New AIIMS - reg.

Sir,

Kind attention is invited to Rule 20 of the CCS (Conduct) Rules, 1964 which envisages that ***No Government servant shall bring or attempt to bring any political or other outside influence to bear upon any superior authority to further his interests in respect of matters pertaining to his service under the Government".***

2 . All Executive Directors are requested to appropriately advise and ensure strict compliance of the above Rule by the employees/staff/officials of their institute .

3. This is issued with the approval of Competent Authority.

Encl: As stated.

Yours faithfully,
Digitally signed by
Taranjeet Singh
Date: 28-01-2025
11:05:47
(Taranjeet Singh)
Under Secretary to the Government of India
Tel:011-23061343

Copy to:
(I) Dy. Directors (Admin), All New AIIMS, for immediate strict compliance.

Rule-20. CANVASSING OF NON-OFFICIAL OR OTHER OUTSIDE INFLUENCE:

No Government servant shall bring or attempt to bring any political or other outside influence to bear upon any superior authority to further his interests in respect of matters pertaining to his service under Government.

Government of India Decisions

(1) Representation on service matters by relatives should be discouraged –

Relatives of a Government servant sometime make representations concerning service matters affecting the Government servant. This is done in some cases in the hope of reviving a representation which the Government servant had himself made and which had been turned down. In some cases, the procedure is resorted to in order to get round the requirements that the Government servant should submit his representation through his official superiors. The practice is obviously undesirable and should be strongly discouraged. It has accordingly been decided that no notice should be taken of a representation on service matters submitted by a relative of a Government servant. The only exception may be cases in which because of the death or physical disability, etc. of the Government servant, it is impossible for the Government servant himself to submit a representation.

[MHA OM No. F25/21/63-Ests.(A), dated 19.09.1963]

(2) Prohibition on brining any political or outside influence in respect of matters pertaining to service under the Government.

Rule 20 of the CCS (Conduct) Rules, 1964 provides that no Government servant shall bring or attempt to bring any political or other outside influence to bear upon any superior authority to further his interest in respect of matters pertaining to his service under the Government. Instructions have been issued from time to time bringing to the notice of all Government servants the aforesaid rule provisions. Instances have come to notice where individual Government servants have approached the Ministry of Urban Development (Directorate of Estate) for out of turn allotment of residential accommodation, or for a departure from the allotment rules through Members of Parliament, prominent persons, politicians etc. Since the allotment of Government accommodation to a Government servant is made only because of his service under the Government, such canvassing for out of turn allotment through MPs and other political persons etc. constitutes a violation of the provisions of Rule 20 of the CCS (Conduct) Rules, 1964. The Government servants are, therefore, advised to refrain from such practice. They should not bring or attempt to bring any political or other out side influence to further their interests in respect of matters pertaining to their service under the Government, including allotment of residential accommodation.

[DOPT OM No. 11013/6/90-Estt.(A), dated 30.03.1990]

(3) Procedure for dealing with the Government servants attempting to further their service interests through non-Governmental influence-instructions with reference to rule 20 of the CCS (Conduct) Rules, 1964-regarding.

Rule 20 of the CCS (Conduct) Rules, 1964 provides that no Government servant shall bring or attempt to bring any political or other outside influence to bear upon any superior authority to further his/her service under the Government. The Government of India has, from time to time, emphasized that Government servants should not approach Members of Parliament or State Legislatures or other

political/outside authorities to sponsor their cases in respect of service matters. As per the existing instructions, vide OM No. 11013/7/85-Estt. (A), dated 22.05.1985, the following action should be taken against Government servants approaching Members of Parliament or State Legislatures for sponsoring individual cases:

(i) A Government employee violating the aforesaid provisions of the Conduct Rules for the first time should be advised by the appropriate disciplinary authority, to desist from approaching Members of Parliament /Members of State Legislature to further his/her interest in respect of matters pertaining to his/her service conditions. A copy of this advice need not, however, be placed in the CR dossier of the employee concerned.

(ii) If a Government employee is found guilty of violating the aforesaid provisions of the Conduct Rules a second time despite the issue of advice on the earlier occasion, a written warning should be issued to him/her by the appropriate disciplinary authority and a copy thereof should be placed in his/her CR dossier.

(iii) If a Government employee is found guilty of violating the aforesaid provisions of the Conduct Rules, despite the issue of warning to him/her, disciplinary action should be initiated against him/her by the appropriate disciplinary authority under the provision of CCS (CCA) Rules, 1965.

2. In spite of these instructions, cases of individual Government servants continue to be sponsored by pubic representatives/outside authorities. After careful consideration of all aspects of the matter it has been decided that the following procedure may be adopted for dealing with communications from public representatives/outside authorities relating to the service matters of Government employees:

(a) Communications received from public representatives regarding problems of groups/categories of Government functionaries must be entertained and dealt with on a time-bound basis. In all such cases, after due examination, appropriate replies would continue to be issued at the level of the Minister concerned.

(b) All communications from public representatives relating to the grievances of the retired personnel should receive the same consideration and be dealt with in the same way as outlined in (a) above.

(c) In cases in which a public representative sponsors the cause of an individual Government servant (e.g. recruitment, appointment, promotion, posting to particular station, appointment to a specific position, complaints against supersession, expunction of adverse remarks, allotment of Government accommodation, etc.) a formal reply should continue to be sent from the Minister acknowledging the receipt of the communication stating that the contents of the letter have been noted and where necessary, suggesting that the person whose case has been recommended, may be advised to represent his case through proper official channels. All such communications addressed to the Minister shall be replied to at, his/her level. In all such cases the formal reply given by the Minister shall be deemed to dispose off the communication unless there are further directions from the Minister in the matter.

[DOPT OM No. 11013/12/94-Estt.(A), dated 12.01.1995]

(4) Canvassing of non-official or other outside influence by Government servants.

As the Ministries/Departments are aware, bringing or attempting to bring any political or other outside influence by a Government servant to bear upon any superior authority to further his interest in respect of service matters pertaining to his service under the Government is prohibited under the provisions of the Conduct Rules. Detailed procedure for dealing with the Government servants attempting to further their service interests through non-Governmental influence has been prescribed in this Department's OM No. 11013/12/94-Estt.(A) dated 12.01.1995.

2. In spite of these instructions, it has come to the notice of this Department that certain Government servants are bringing to bear outside influence indirectly to further their service interests. It is clarified that brining of indirect influence by Government servant would also attract the provisions of rule 20 of the CCS (Conduct) Rules, 1964.

3. All Ministries/Departments/Offices etc. are requested to bring the existing instructions/rules to the notice of all concerned under their control and to take effective action against the Government servants who bring or attempt to bring outside influence to further their service interests, as prescribed in the OM dated 12.01.1995.

[DOPT OM No. 11013/11/97-Estt.(A), dated 06.11.1997]

(5) Representation from Government servants on service matters.

It has been envisaged in the Ministry of Home Affairs OM No. 118/52-Ests. Dated 30th April 1952 on the subject mentioned above (copy enclosed for ready reference) that whenever, in any matter connected with his service rights or conditions, a Government servant wishes to press a claim or to seek redress of a grievance, the proper course for him is to address his immediate official superior, or the Head of his office, or such other authority at the lowest level as he is competent to deal with the matter. Of late, it is observed that there has been a tendency on the part of officers at different levels to bypass the prescribed channels of representation and write directly to the high functionaries, totally ignoring the prescribed channels. The problem is more acute in large Departments where often very junior employees at the clerical level address multiple representations to the Minister, Prime Minister and other functionaries. Apart from individual representations, the service unions have also developed a tendency to write to the Ministers and Prime ministers on individual grievances. Some of these representations are often forwarded through Members of Parliament, in violation of Rule 20 of the CCS (Conduct) Rules, 1964.

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Request for additional land for expansion of AIIMS- reg.

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, Dec 18, 2025 at 11:01 AM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

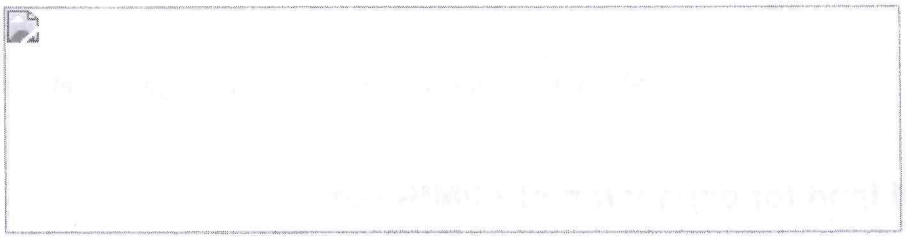
Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **Mr Sourabh** <pmssy5-mohfw@gov.in>
Date: Fri, Jan 31, 2025 at 5:14 PM
Subject: Request for additional land for expansion of AIIMS- reg.
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Executive Director Raebareli <ed.aiimsrbl@gmail.com>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, Dinesh Singh <director@aiimsbathinda.edu.in>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, Director AIIMS Madurai <drmhraosvims1957@gmail.com>, ED AIIMS Guwahati <executive-director@aiimsguwahati.ac.in>, ED AIIMS Bilaspur <edaiimsbls@gmail.com>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Director AIIMS Vijaypur <shakti810505@gmail.com>, DDA AIIMS Awantipora <rakeshkumar7123@yahoo.in>, Executive Director AIIMS Rajkot <ed.aiimsrajkot@gmail.com>, Director AIIMS Bibinagar <director.aiimsbbnagar@gmail.com>, Executive Director AIIMS Darbhanga <madhabananda@gmail.com>
Cc: DDA BHOPAL <dydir@aiimsbhopal.edu.in>, DDA Bhubaneswar <dda@aiimsbhubaneswar.edu.in>, DDA Jodhpur <dda@aiimsjodhpur.edu.in>, DDA AIIMS Patna <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, DDA AIIMS Rishikesh <dda@aiimsrishikesh.edu.in>, DDA RAEBARELI <ddaaiimsrbl@gmail.com>, DDA MANGALAGIRI <dda@aiimsmangalagiri.edu.in>, DDA NAGPUR <dda@aiimsnagpur.edu.in>, Dr. DDA AIIMS Kalyani <kpradip10@gmail.com>, AIIMS DDA Gorakhpur <dda@aiimsgorakhpur.edu.in>, DDA AIIMS Bathinda <rajeevsenroy30@gmail.com>, DDA AIIMS Guwahati <dda@aiimsguwahati.ac.in>, DDA AIIMS BILASPUR <dda@aiimsbilaspur.edu.in>, dda bilaspur <ddaaiimsbilaspur@gmail.com>, DDA AIIMS Deoghar AIIMS Deoghar <dda@aiimsdeoghar.edu.in>, DDA AIIMS Vijaypur, Jammu <ddaaiimsjammu@gmail.com>, DDA AIIMS Awantipora <rakeshkumar7123@yahoo.in>, DDA AIIMS Madurai <ddamadurai1189@gmail.com>, DDA AIIMS Rajkot <dda.aiimsrajkot@gmail.com>, DDA AIIMS BIBINAGAR <dda.aiimsbibinagar@gmail.com>, Phool Chandra Prasad <prasad-upsc@gov.in>, Dharm Bir Kumar SIngh <dharmbk.singh@nic.in>, Sourabh <sourabh.12@gov.in>, NARVEER REDHU <narveer.redhu@gov.in>

Respected Sir/Madam,

With reference to the subject cited above, Please find the attachment herewith.

Regards
PMSSY-V Section
Ministry of Health and Family Welfare



Letter dated 31-1-25.pdf
84K

File No.: Z-28016/242/2024-PMSSY-V (8311298)
Government of India
Ministry of Health & Family Welfare
Department of Health & Family Welfare
(PMSSY-V Section)

Nirman Bhawan, New Delhi-11
Date: 31-01-2025

To
The Executive Director,
[All AIIMS under PMSSY]

Subject: Request for additional land for expansion of AIIMS- reg.

Sir/Madam,

It has come to the notice of this Ministry that Executive Directors AIIMS are directly writing letters to the Chief Minister and Chief Secretary of their respective States for allotment of additional land to AIIMS for expansion of the facilities without specific approval of the Ministry .

2. Since construction of new facilities requires adequate planning, provisioning of funds, creation of posts etc, all the Executive Directors, AIIMS are accordingly advised to correspond with the State Governments for allotment of additional land only after specific approval of the Ministry .

Yours faithfully,
Digitally signed by
Dharm Bir Kumar Singh
Date: 31-01-2025
16:14:19
(Dharm Bir Kumar Singh)
Under Secretary to Govt. of India
Tele: 011-23060006

Encl. as above

Copy to:

Deputy Director Administration, All AIIMS under PMSSY.

Copy for information to:

Dir. / DS (PMSSY-I/II/III/IV & V).

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Most Immediate: Periodic review of central government employees for strengthening of administration under FR 56 (j) and Rule 48 of CCS (Pension) Rule, 1972 [now, revised as rule of CCS (Pension) Rules, 2021]-reg. .

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, Dec 18, 2025 at 11:00 AM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **pmssysection iv** <pmssysectioniv@gmail.com>
Date: Thu, Feb 6, 2025 at 3:34 PM
Subject: Most Immediate: Periodic review of central government employees for strengthening of administration under FR 56 (j) and Rule 48 of CCS (Pension) Rule, 1972 [now, revised as rule of CCS (Pension) Rules, 2021]-reg. .
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, Executive Director Raebareli <edaiimsrbl@gmail.com>, <rajwanshiarvind@hotmail.com>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, <madhabananda@gmail.com>, <sachimohanty@rediffmail.in>
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, <DDA@aiimsrbl.edu.in>, Dr. PRADIP KUMAR <kpradip10@gmail.com>, <dda@aiimskalyani.edu.in>, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, Rajeev Sen Roy <rajeevsenroy30@gmail.com>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, <dda@aiimsbilaspur.edu.in>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, <sanjaygarg0204@yahoo.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, Administrative Officer <ao.aiimsmadurai@gmail.com>, T Ngamlien <t.ngamlien@icg.gov.in>, Mukesh Kumar <mac.prasad@gmail.com>, <ddaaiimsawantipora1@gmail.com>, Dy Director Administration AIIMS, Raebareli <ddaaiimsrbl@gmail.com>, Cc: <Dinesh.kumar14@nic.in>, : <Ak.biswas57@nic.in>, Taranjeet Singh <taranjeet.singh@nic.in>, Suprava Poddar <sup15.81997@gov.in>, <ankit.vyas@gov.in>, <pandey.ujjwal@gov.in>

MOST IMMEDIATE

Sir/ Madam

Please find attached herewith a copy of letter dated 6th February, 2025 on the above cited subject matter. It has been observed that only a few AIIMS are submitting timely information on the subject matter. It is

therefore, once again requested to provide the requisite information on the matter to this Division in prescribed format as mentioned in our earlier letter dated 12.12.2024 in a timely manner preferably in the first week of every month without fail only to the below mentioned email IDs. The information will be compiled in this Division and thereafter action will be taken.

Thanks and regards.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officials of PMSSY-IV Section at - dinesh.kumar14@nic.in; ak.biswas57@nic.in; taranjeet.singh@nic.in; ; sup15.81997@gov.in;

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

---

3 attachments

Letter (83).pdf
95K

Encl (24).pdf
60K

ENCL2ltrdtd121224.pdf
262K

No.: -28016/66/2024-PMSSY-IV

Government of India

Ministry of Health and Family Welfare

(PMSSY - IV Section)

***

Room No:745A, Nirman Bhawan, New Delhi

Dated 6th February,2025

To

Executive Director, All New AIIMS

Subject: Periodic review of central government employees for strengthening of administration under FR 56 (j) and Rule 48 of CCS (Pension) Rule, 1972 [now, revised as rule of CCS (Pension) Rules, 2021]-reg. -Reg.

Sir,

I am directed to refer this section's letter of even number dated 12.12.2024 on the subject mentioned above. In this connection it is to mention that only a few AIIMS are sending information on regular basis in the subject matter. It is therefore, once again requested to provide the requisite information in prescribed format to the PMSSY Division preferably in the first week every month without fail so that the same can be compiled and send to the concerned Section of this Ministry for further necessary action at their end.

2. This issues with the approval of the competent authority.

Encl(1): As above.

Yours faithfully,

Digitally signed by Taranjeet Singh
Date: 06-02-2025 14:38:07

(Taranjeet Singh)

Under Secretary to the Government of India

Tel:011-23061343

Copy to:

(I) Dy. Director (Admin), All New AIIMS, for strict compliance.

(II) Section Officer, Establishment-I section, MoHFW

No.: -28016/66/2024-PMSSY-IV
Government of India
Ministry of Health and Family Welfare
(PMSSY - IV Section)
***

Room No:745A, Nirman Bhawan, New Delhi

Dated 12th December, 2024

To

Executive Director, All New AIIMS except AIIMS,Raebareli, Gorakhpur, Guwahati, Madurai, Mangalagiri, Patna

Subject: Periodic review of central government employees for strengthening of administration under FR 56 (j) and Rule 48 of CCS (Pension) Rule, 1972 [now, revised as rule of CCS (Pension) Rules, 2021]-reg. -Reg.

Sir,

I am directed to forward herewith an e-mail and its subsequent reminders received from Establishment – I Section of MoHFW on the subject cited above.

2. In this regard, it is to inform that All new AIIMS have been requested several times via different mode of communications including emails , whatsapp group reminders, telephone etc. to provide the requisite information in the revised format. However, information has been received from only few AIIMS. This has been viewed seriously by the Competent Authority.

3. Keeping in view the position mentioned in para '2' above, it is advised to provide above mentioned information to this Ministry with in a period of three (3) days failing which responsibility of the concerned officer/s shall be fixed for non-compliance of the directions of this Department.

4. This issues with the approval of the competent authority.

Encl(1): As above.

Yours faithfully,

Signed by Taranjeet Singh
Date: 12-12-2024 10:34:54

(Taranjeet Singh)
Under Secretary to the Government of India
Tel:011-23061343

Copy to:

(I) Dy. Director (Admin), All New AIIMS, for strict compliance.
(II) Section Officer, Establishment-I section, MoHFW

Email **Suprava Poddar**

Fwd: REMINDER 2 : Information on Periodic Review of Central Government Employees under Fundamental Rule (FR) 56(j) from 01.04.2024 to Till date -reg.

From : Vaishali Vinayak <vaishali.vinayak@gov.in> Mon, Dec 09, 2024 11:28 AM

Subject : Fwd: REMINDER 2 : Information on Periodic Review of Central Government Employees under Fundamental Rule (FR) 56(j) from 01.04.2024 to Till date -reg.

To : Suprava Poddar <sup15.81997@gov.in>

Please put up the matter on priority.

========== Forwarded message ==========
From: Ujjwal Pandey <pandey.ujjwal@gov.in>
To: "Dinesh Kumar"<dinesh.kumar14@nic.in>
Cc: "neelamchachra"<neelam.chachra@nic.in>, "ankitaedu"<ankita.edu@nic.in>, "ANKITA MISHRA BUNDELA"<js-pmssy-mohfw@gov.in>, "taranjeetsingh" <taranjeet.singh@nic.in>, "akbiswas57"<ak.biswas57@nic.in>, "section-ini1-mohfw" <section-ini1-mohfw@gov.in>, "shankargarg"<shankar.garg@gov.in>, "Amit Batra" <amit.batra@gov.in>, "Vaishali Vinayak"<vaishali.vinayak@gov.in>
Date: Mon, 09 Dec 2024 10:32:32 +0530
Subject: Fwd: REMINDER 2 : Information on Periodic Review of Central Government Employees under Fundamental Rule (FR) 56(j) from 01.04.2024 to Till date -reg.
========== Forwarded message ==========

REMINDER 2

Madam/Sir

With reference to the trail mail dated 27.11.2024, the requisite information in respect of **All AIIMS** is still awaited. Therefore, it is again requested to send the **consolidated information** of all the AIIMS at the earliest.

Regards

Ujjwal Pandey
Assistant Section Officer
Estt-1, MoHFW

========== Forwarded message ==========
From: Ujjwal Pandey <pandey.ujjwal@gov.in>
Cc: "neelamchachra"<neelam.chachra@nic.in>, "ankitaedu"<ankita.edu@nic.in>, "ANKITA MISHRA BUNDELA"<js-pmssy-mohfw@gov.in>, "taranjeetsingh" <taranjeet.singh@nic.in>, "akbiswas57"<ak.biswas57@nic.in>, "section-ini1-mohfw"

<section-ini1-mohfw@gov.in>, "shankargarg"<shankar.garg@gov.in>, "Amit Batra" <amit.batra@gov.in>, "Vaishali Vinayak"<vaishali.vinayak@gov.in>
Date: Fri, 06 Dec 2024 12:15:11 +0530
Subject: REMINDER 1 : Information on Periodic Review of Central Government Employees under Fundamental Rule (FR) 56(j) from 01.04.2024 to Till date -reg.
========== Forwarded message ==========

REMINDER 1

Madam/Sir

With reference to the trail mail dated 27.10.2024, the requisite information in respect of **All AIIMS** is still awaited. Therefore, it is again requested to send the **consolidated information** of all the AIIMS at the earliest.

Regards

Ujjwal Pandey
Assistant Section Officer
Estt-1, MoHFW

========== Forwarded message ==========
From: Ujjwal Pandey <pandey.ujjwal@gov.in>
To: "Dinesh Kumar"<dinesh.kumar14@nic.in>
Cc: "neelamchachra"<neelam.chachra@nic.in>, "ankitaedu"<ankita.edu@nic.in>, "ANKITA MISHRA BUNDELA"<js-pmssy-mohfw@gov.in>, "taranjeetsingh" <taranjeet.singh@nic.in>, "akbiswas57"<ak.biswas57@nic.in>, "section-ini1-mohfw" <section-ini1-mohfw@gov.in>, "shankargarg"<shankar.garg@gov.in>, "Amit Batra" <amit.batra@gov.in>, "Vaishali Vinayak"<vaishali.vinayak@gov.in>
Date: Thu, 05 Dec 2024 12:14:31 +0530
Subject: Information on Periodic Review of Central Government Employees under Fundamental Rule (FR) 56(j) from 01.04.2024 to Till date -reg.
========== Forwarded message ==========

Madam/Sir

With reference to the trail mail dated 27.10.2024, the requisite information in respect of **All AIIMS** is still awaited. Therefore, it is again requested to send the **consolidated information** of all the AIIMS at the earliest.

Regards

Ujjwal Pandey
Assistant Section Officer

Estt-1, MoHFW

========== Forwarded message ==========
From: Ujjwal Pandey <pandey.ujjwal@gov.in>
To: "Neelamchachra"<Neelam.chachra@nic.in>, "Taranjeetsingh" <Taranjeet.singh@nic.in>, "Akbiswas57"<Ak.biswas57@nic.in>, "Amit Sharma" <amitkumar.sharma@gov.in>, "aditibhatia52"<aditi.bhatia52@nic.in>, "shambhukumar" <shambhu.kumar@nic.in>, "sidhurajender"<sidhu.rajender@nic.in>, "Anuradharamakrishan"<Anuradha.ramakrishan@nic.in>, "Abhishekpandey86" <Abhishek.pandey86@nic.in>, "Anuragtiwari86"<Anurag.tiwari86@nic.in>, "Rajnibala18" <Rajni.bala18@gov.in>, "Bikashmahato"<Bikash.mahato@nic.in>, "Hemrajmeena13" <Hemraj.meena13@nic.in>, "Rajeshk93"<Rajesh.k93@nic.in>, "Rajeshkumar26" <Rajesh.kumar26@nic.in>, "Sushilmishra"<Sushil.mishra@nic.in>, "Ranjandoley90" <Ranjan.doley90@nic.in>, "nikhilbhatnagar"<nikhil.bhatnagar@gov.in>, "shubhenduss" <shubhendu.ss@nic.in>, "Lavkeshsehgal79"<Lavkesh.sehgal79@nic.in>, "pamposhpokhriyal"<pamposh.pokhriyal@nic.in>
Cc: "section-ini1-mohfw"<section-ini1-mohfw@gov.in>, "shankargarg" <shankar.garg@gov.in>, "Amit Batra"<amit.batra@gov.in>, "Vaishali Vinayak" <vaishali.vinayak@gov.in>, "Prerna ."<arora.prerna@gov.in>, "PRERNA"<so.ini2-mohfw@gov.in>, "ADITYA LOHIA"<aditya.lohia@nic.in>, "MANTU KUMAR" <mantu.kumar84@nic.in>, "hospital2section"<hospital2section@gmail.com>, "Vivekmishra92"<Vivek.mishra92@gov.in>, "Hospital-I Section"<hospital1.sec-mohfw@gov.in>, "ncdcellmohfw"<ncdcellmohfw@gmail.com>, "ANKIT KUMAR" <nesection-mohfw@gov.in>, "Shashank Shekhar"<mentalhealth-mohfw@gov.in>, "Drugs Regulation Section"<drugsdiv-mohfw@gov.in>, "vaccineinstitute" <vaccine.institute@gmail.com>, "rajneeshdixit91"<rajneesh.dixit91@nic.in>, "ncd2mohfw"<ncd2mohfw@gov.in>, "sandeep dhanda"<dhanda.sandeep@gov.in>, "SUMIT KUMAR"<sumit.kumar13@nic.in>, "SUMIT KUMAR"<food-mohfw@gov.in>, "adminad1"<admin.ad1@nha.gov.in>, "mep2section"<mep2section@gmail.com>, "Procurement I EPW Section"<epwsec-mhfw@nic.in>, "Sharmiladevik" <Sharmila.devik@nic.in>, "Sordcell2"<So.rdcell2@gmail.com>, "Rlmeena39" <Rl.meena39@nic.in>, "Phihsection"<Phih.section@gov.in>, "Sunilmandi" <Sunil.mandi@nic.in>, "Akshaykumar89"<Akshay.kumar89@gov.in>, "Clddghs23" <Clddghs23@gmail.com>, "officememo597"<officememo597@gmail.com>
Date: Wed, 27 Nov 2024 10:32:07 +0530
Subject: Information on Periodic Review of Central Government Employees under Fundamental Rule (FR) 56(j) from 01.04.2024 to Till date -reg
========== Forwarded message ==========

Madam/Sir

It is requested to furnish the following information in respect of Attached offices/ Subordinate offices/ Autonomous bodies/ Statutory bodies/ PSUs/ Banks/ etc under administrative control of divisions by 5 **PM 27.11.2024** on email : **pandey.ujjwal@gov.in, pankaj.verma28@nic.in**

(A) Consolidated data on FR 56(j)/ similar provisions (in respect of Main Secretariat/ Attached Offices / Subordinate offices/ Autonomous bodies/ Statutory bodies)

Data from 01.04.2024 to till date					
No. of employees reviewed			No. of employees retired		
Group A	Group B	Group C	Group A	Group B	Group C

(B) Information of CPSEs of Ministries/ Departments invoking similar provisions during the period.

S.No.	Name of the CPSE	Reviewed		Retired	
1.		Executive	Non-executive	Executive	Non-executive
2.					

(C) Apart from this, information on employees who have been compulsorily retired/ removed/ dismissed from service etc. During the period: -

S.No.	Name of Ministry	Group A	Group B	Group C
1.				
2.				

2. Further, it is stated that the data submitted by Divisions through is not at all in sync with the data posted on the probity portal which is causing confusion. Therefore, all the divisions are requested to kindly re-check their data posted on Probity Portal and get it updated .

Regards

Ujjwal Pandey
Assistant Section Officer
Estt-1, MoHFW

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Circulation of proposed guidelines for the use of Internal Resources in all new AIIMS/ INIs/ Institutes/ Hospitals of the Ministry - seeking comments/ suggestions. – reg.

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, Dec 18, 2025 at 10:57 AM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **Director .** <director@aiimspatna.org>
Date: Tue, Feb 11, 2025 at 11:15 AM
Subject: Fwd: Circulation of proposed guidelines for the use of Internal Resources in all new AIIMS/ INIs/ Institutes/ Hospitals of the Ministry - seeking comments/ suggestions. – reg.
To: DDA AIIMS PATNA <dda@aiimspatna.org>, Finance & Chief Accounts Officer <fcao@aiimspatna.org>

Sd/-
Prof. (Dr.) Saurabh Varshney
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109

---------- Forwarded message ---------
From: **pmssysection iv** <pmssysectioniv@gmail.com>
Date: Tue, Feb 4, 2025 at 12:58 PM
Subject: Circulation of proposed guidelines for the use of Internal Resources in all new AIIMS/ INIs/ Institutes/ Hospitals of the Ministry - seeking comments/ suggestions. – reg.
To: Jaideep Kumar Mishra <Asfa-mhfw@nic.in>, j_mishra <j_mishra@gov.in>, ROLI SINGH <asfr-mohfw@gov.in>, Roli Singh <roli.singh@ias.nic.in>, Roli Singh <ash-mohfw@nic.in>, Ms. V Hekali Zhimomi <Zhimomiv@ias.nic.in>, Ms. V. Hekali Zhimomi <Dgoffice@naco.gov.in>, L Sweety Changsan <lschangsan@nic.in>, Aradhana Patnaik <asmd-mohfw@nic.in>, Dr. Manashvi kumar <jstraining-mohfw@gov.in>, Pushpendra Rajput <Pushpendra.r@nic.in>, Vandana Jain <Vandana.jain@nic.in>, Elangbam Robert Singh <Robert.elangbam@gov.in>, Vijay Kumar Sinha <Sinha.vijay@nic.in>, Indrani Kaushal <Ea-mohfw@nic.in>, Dr. K. K. Tripathy <kk.tripathy@nic.in>, RAJIV WADHAWAN <r.wadhawan15@nic.in>, Ms Meera Srivastava <jsrch-mohfw@gov.in>, Smt. Jaspal Kaur <cca-mohfw@nic.in>, Anoop Kumar Puri <anoopk.puri@nic.in>, <Ddgtb@rntcp.org>, Pradeep Khasnobis <pradeep.khasnobis@gov.in>, ANKITA MISHRA BUNDELA <js-pmssy-mohfw@gov.in>, Saurabh Jain <js-publichealth@gov.in>, ANKITA MISHRA BUNDELA <Ankita.edu@nic.in>, Prof (Dr) Atul Goel <dghs@nic.in>
Cc: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, Executive Director Raebareli <edaiimsrbl@gmail.com>, <rajwanshiarvind@hotmail.com>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, Prof. Dr. D.K. Singh, Director <director@aiimsbathinda.in>, Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>,

<shakti810505@gmail.com>, <cdskatoch@gmail.com>, Executive Director AIIMS Rajkot <ed.aiimsrajkot@gmail.com>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, <madhabananda@gmail.com>, <sachimohanty@rediffmail.in>, Dr Vivek Lal <dpgi@pgimer.edu.in>, <director@jipmer.ac.in>, Srinivas.M <director@aiims.gov.in>, Director Neigrihms <director-neigrihms@gov.in>, <nalinaiims.mehta@gmail.com>, <eigasunil@gmail.com>, <director@ripans.ac.in>, MS OFFICE SJH <msoffice@vmmc-sjh.nic.in>, Dr. Sunita Sharma <director-lhmc@gov.in>, minakshi Bhardwaj <med.sup@rmlh.nic.in>, Apurva Chandra <secyhfw@nic.in>, Praveen Batra <Praveen.batra@gov.in>, Cc: <dinesh.kumar14@nic.in>, : <ak.biswas57@nic.in>, Mr.SankarGarg Mr.SankarGarg <sankar.garg@gov.in>, Amit Batra <amit.batra@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officials of PMSSY-IV Section at - dinesh.kumar14@nic.in; ak.biswas57@nic.in; sankar.garg@gov.in; amit.batra@gov.in

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

2 attachments

Office Order (11).pdf
95K

Encl dt 14.10.2024.pdf
429K

Reminder

Z-28016/35/2024-PMSSY-IV(8285627)
Government of India
Ministry of Health & Family Welfare
(PMSSY-IV Section)

Room No. 745-A, Nirman Bhawan, New Delhi
Dated the 03-02-2025

Office Order

Subject: Circulation of proposed guidelines for the use of Internal Resources in all new AIIMS/ INIs/ Institutes/ Hospitals of the Ministry - seeking comments/ suggestions. – reg.

This Division vide office order of even no dated 14.10.2024 had circulated proposed guidelines for the use of Internal Resources in all new AIIMS/ INIs/ Institutes/ Hospitals of the Ministry for seeking comments/ suggestions by 28.10.2024. The same have been received only from 11 Institutes/ Division viz - AIIMS Bhopal, AIIMS Bhubaneswar, NHM-Finance Division, AIIMS Raebareli, RIMS Imphal, AIIMS New Delhi, AIIMS Madurai, AIIMS Awantipora, AIIMS Deoghar, AIIMS Nagpur, AIIMS Patna.

2. All the remaining Institutes/ Divisions are requested to provide comments/ suggestions at the earliest.

Digitally signed by
ARUN KUMAR BISWAS
Date: 03-02-2025
20:16:41

(Arun Kumar Biswas)
Under Secretary to the Govt. of India
Tel:011-23061343

Encl(1): Office order of even no dated 14.10.2024

To

i. All Additional Secretaries/ Joint Secretaries, MoHFW – with a request to circulate the proposed Guidelines to all the Institutes/ Hospitals/ Autonomous Bodies under their administrative control.

ii. Director General of Health Services, MoHFW, GoI

iii. AS&FA, MoHFW

Copy to :

i. Director, AIIMS New Delhi

ii. Director, PGIMER, Chandigarh,

iii. Director, JIPMER, Puducherry

iv. Director, NIMHNAS, Bengaluru

v. The Directors/ Executive Directors of new AIIMS under PMSSY

vi. The Directors of Central Government Hospitals in Delhi/ North East Hospitals

Copy for information to :

i. PSO to Secretary(HFW)

ii. PPS to Joint Secretary (PMSSY)

iii. PS to Director (PMSSY-IV)

Z-28016/35/2024-PMSSY-IV(8285627)

Government of India

Ministry of Health & Family Welfare

(PMSSY-IV Section)

Room No. 745-A, Nirman Bhawan, New Delhi

Dated the 14-10-2024

Office Order

Subject: Circulation of proposed guidelines for the use of Internal Resources in all new AIIMS/ INIs/ Institutes/ Hospitals of the Ministry - seeking comments/ suggestions. – reg.

This Ministry vide Office Order dated 22.4.2024, constituted a committee to examine the subject of use of Internal Resources for Financial Management with the objective to lay down Guidelines for the use of Internal Revenue generated by the Institutes for their judicious utilization for enhancing patient care services, promotion of research and innovation and employee and student welfare etc.

2. The committee has submitted its report. The report was examined by this Division in consultation with Internal Finance Division (IFD), MoHFW. The Guidelines emerging out of such examination, are enclosed herewith.

3. **As advised by Secretary Health all AIIMS/ INIs/ Institutes/ Hospitals of the Ministry, all Divisional Heads and IFD are requested to examine the guidelines and share the comments/ suggestions to the Ministry at the earliest latest by 28th Oct 2024 to enable this Division to proceed ahead in the matter .**

Signed by
Arun Kumar Biswas
Date: 14-10-2024 19:05:38
(Arun Kumar Biswas)
Under Secretary to the Govt. of India
Tel:011-23061343

Encl(1): Report/ guidelines for the use of Internal Resources in all new AIIMS/ INIs/ Institutes/ Hospitals of the Ministry

To

i. All Additional Secretaries/ Joint Secretaries, MoHFW – with a request to

circulate the proposed Guidelines to all the Institutes/ Hospitals/ Autonomous Bodies under their administrative control.

ii. Director General of Health Services, MoHFW, GoI
iii. AS&FA, MoHFW

Copy to :

i. Director, AIIMS New Delhi
ii. Director, PGIMER, Chandigarh,
iii. Director, JIPMER, Puducherry
iv. Director, NIMHANS, Bengaluru
v. The Directors/ Executive Directors of new AIIMS under PMSSY
vi. The Directors of Central Government Hospitals in Delhi/ North East Hospitals

Copy for information to :

i. PSO to Secretary(HFW)
ii. PPS to Joint Secretary (PMSSY)
iii. PS to Joint Director (PMSSY-IV)

Gmail

pmssysection iv <pmssysectioniv@gmail.com>

Circulation of proposed guidelines for the use of Internal Resources in all new AIIMS/ INIs/ Institutes/ Hospitals of the Ministry - seeking comments/ suggestions. – reg.

1 message

pmssysection iv <pmssysectioniv@gmail.com> Tue, Oct 15, 2024 at 12:36 PM
To: Asfa-mhfw@nic.in, j_mishra@gov.in, asfr-mohfw@gov.in, Roli Singh <roli.singh@ias.nic.in>, ash-mohfw@nic.in, Zhimomiv@ias.nic.in, Dgoffice@naco.gov.in, lschangsan@nic.in, asmd-mohfw@nic.in, jstraining-mohfw@gov.in, Pushpendra.r@nic.in, Vandana.jain@nic.in, Robert.elangbam@gov.in, Sinha.vijay@nic.in, Ea-mohfw@nic.in, kk.tripathy@nic.in, r.wadhawan15@nic.in, jsrch-mohfw@gov.in, cca-mohfw@nic.in, anoopk.puri@nic.in, Ddgtb@rntcp.org, pradeep.khasnobis@gov.in, js-pmssy-mohfw@gov.in, js-publichealth@gov.in, Ankita.edu@nic.in, dghs@nic.in
Cc: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, edaiimsrbl@gmail.com, rajwanshiarvind@hotmail.com, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, "Prof. Dr. D.K. Singh, Director" <director@aiimsbathinda.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, shakti810505@gmail.com, cdskatoch@gmail.com, Executive Director AIIMS Rajkot <ed.aiimsrajkot@gmail.com>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, madhabananda@gmail.com, sachimohanty@rediffmail.in, Dr Vivek Lal <dpgi@pgimer.edu.in>, director@jipmer.ac.in, director@aiims.gov.in, Director Neigrihms <director-neigrihms@gov.in>, nalinaiims.mehta@gmail.com, eigasunil@gmail.com, director@ripans.ac.in, MS OFFICE SJH <msoffice@vmmc-sjh.nic.in>, "Dr. Sunita Sharma" <director-lhmc@gov.in>, minakshi Bhardwaj <med.sup@rmlh.nic.in>, secyhfw@nic.in, Praveen.batra@gov.in, "Cc:" <dinesh.kumar14@nic.in>, ":" <ak.biswas57@nic.in>, sankar.garg@gov.in, Amit Batra <amit.batra@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officials of PMSSY-IV Section at - dinesh.kumar14@nic.in; ak.biswas57@nic.in; sankar.garg@gov.in; amit.batra@gov.in
Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

2 attachments

Office Order 2.pdf
81K

encl.docx
28K

Proposed guidelines for the use of Internal Resources in all new AIIMS/ INIs/ Institutes/ Hospitals of the Ministry

The General Financial Rules lay down the principles for setting up of Autonomous Organizations and their fund management. The Guidelines will be operational within the ambit of the GFRs.

As per Rule 229 (iv) states that All autonomous organizations, new or already in existence should be encouraged to maximize generation of internal resources and eventually attain self-sufficiency.

Rule 229 (v) provides that the Ministry or Department may consider creating a Corpus Fund for an Autonomous Body only with prior concurrence of Ministry of Finance if the corpus is created out of budgetary allocation. If the corpus is created out of internal accruals of the body, approval of the administrative Ministry must be obtained.

2. The major source of Internal Revenue Generation include :

Heads	Description
Hospital	a. User Fees: Patient Registration, Day-Care & Indoor Admission Fees, Bed Charges (General Ward) & Room Rent (Private Ward), OT Charges for procedures & surgeries, Pathological & Radiological investigations. b. Service charges: Vaccination, Mortuary, Embalming, etc. c. Pharmacy Charges: Implants, vaccines, Drugs, etc. d. Insurance claims: TPA, CGHS, etc. e. AB-PMJAY reimbursements.
Academic Fees	a. Admission fees from students/ trainees/fellowship programmes. b. Unspent balance of various workshops/ training programmes. c. Externships. d. Auditorium charges.

Research Grant	a. Collaborations with external agencies to create new commercialized products, like rapid diagnostic tests etc. b. Patent charges. c. Overhead charges from External Research Projects
Examination Fees	a. Examination fees from applicants for recruitments. b. National Exams like NEET, NORCET etc.
Any Other	CSR/ Philanthropy and Donation Any Other a. Start-ups in the Institutes. b. Penalty charges from defaulter firms/vendors c. Penalty from students & staff d. Sale of scrap material. e. Rental charges (shops, ATMs, parking, canteen etc.). f. Collection on account of shortfall in notice period of employees resigning. g. Electricity & water charges from various vendors and contractors (Engineering works). h. Interest earned from internal receipts savings bank account & Fixed Deposits & Security Deposits of tenders. i. Income from Guest house receipts.

3. In accordance with the recommendation of the committee set up the Ministry on the above subject the internal revenue of the Institute can be broadly utilized for the following purpose and in the proportion indicated:

3.1 Patient Welfare (50% ± 5%)

1. **To support emergency health** care needs within the institution.

2. **To undertake Community Outreach activities for** extending healthcare services to the broader community.

3. **Patient Welfare Activities designed to improve the well-being and comfort of patients and their attendants by** development of facilities such as Vishram Sadans (rest houses), waiting halls, cafeterias, access to clean drinking water, play areas and libraries for children etc.

4. **Patient Navigation Services** to guide patients and their families through the complex healthcare system through intra-hospital navigation app /engaging volunteers etc.

5. **Quality Improvement Initiatives including** Accreditation programs such as NABH (National Accreditation Board for Hospitals & Healthcare Providers), NQAS (National Quality Assurance Standards), and NABL (National Accreditation Board for Testing and Calibration Laboratories)

6. **Innovation and Pilots:** for advancing healthcare practices and exploring new approaches to patient care. These initiatives may include testing new technologies, treatment protocols, and service delivery models on a small scale before broader implementation.

7. **Health Education and Awareness Programs** for patients and their families to enhance their understanding of health conditions, treatment options, and preventive measures.

8. **Holistic Health Support:** Providing mental health services, counselling complementary therapies such as yoga, meditation, acupuncture, and music therapy to support traditional medical treatments and improve patient well- being.

9. **Support for Chronic Disease Management for diseases** such as diabetes, hypertension, heart disease, through regular medication management, and lifestyle coaching.

10. **Rehabilitation Services:** such as physical therapy, occupational therapy, and speech therapy to aid in the recovery and improve the quality of life for patients with disabilities or those recovering from surgeries and illnesses.

11. **Palliative and End-of-Life Care** for patients with life-limiting illnesses, focusing on pain relief, emotional support etc.

12. **Establishing mechanisms for Feedback and Patient Advocacy** to ensure that the patient's voice is heard, and their rights are protected within the healthcare system.

13. **Volunteer Programs** where community members can contribute their time and skills to support various patient welfare activities

14. **Promotion of Digital Health through use of** ABDM , mobile apps, telemedicine, patient portals and other platforms /apps

15. **Cultural and Recreational Activities** within the hospital to provide emotional relief and improve the morale of patients.

3.2 Employee Welfare **(20% ± 5%)**

1. **Promoting Team Building and Enhancing Motivation through workshops, trips etc. Investing in tools and technologies that facilitate better collaboration and communication among team members.**
2. **Recreational Activities like Annual Sports/Cultural Programs** for fostering a positive and inclusive workplace culture, encouraging physical fitness, fostering creativity and talent and improving work life balance.
3. **Faculty and Student Exchange Programme for Networking and Learning Best Practices.**
4. **Professional Development Programs** including workshops, seminars, online courses, and certification programs to enhance the skills and knowledge of employees.
5. **Health and Wellness Programs** to promote the physical and mental well- being of employees.
6. **Employee Recognition and Reward Programs** to acknowledge and appreciate the hard work and achievements of employees.
7. **Counselling and Support Services to help** employees to deal effectively with personal or work-related issues. Implementing programs to identify, prevent, and manage burnout among healthcare workers,
8. **Ensuring Safety and Ergonomics** by conducting regular safety audits, providing ergonomic workstations, offering training on workplace safety practices etc.
9. **Team Collaboration Tools:** such as project management software, instant messaging platforms, and video conferencing tools.
10. **Support for Shift Workers:** Providing specialized support for employees working in shifts, such as sleep management programs, healthy meal options available at all hours, and flexible scheduling to reduce fatigue.
11. **Crisis Management Training:** Providing training on crisis management, including handling medical emergencies, natural disasters etc.
12. **Wellness Rooms and Rest Areas:** Creating dedicated wellness rooms and rest areas within the hospital where staff can take breaks, relax, and recharge during their shifts.
13. No Allowances to be paid to employees out of the Internal Revenue

3.3 Academic and Research Welfare (20% ± 5%)

1. **Scholarships** to students for extra trainings courses andresearch.

2. **Academic trips and Faculty Exchange programme** to other institutes to understand best practices, to promote cross-pollination of ideas, collaborative research, and exposure to diverse teaching and research practices.

3. Mess facility for economically weak students or any other help required as deemed fit by Director.

4. **Conference Sponsorships for** national and international conferences for faculty, residents, and students to present their research findings.

5. **Professional Development Workshops** on research methodologies, research ethics, regulatory compliance, scientific writing, and data analysis to enhance the research skills of faculty and students.

6. **Facilitate Collaboration with Industry and Academia** to promote joint research projects, internships, and academic exchange programs.

7. **Publication Support** for the publication of research findings in reputed journals.

8. **Seed Funding for** healthcare-related startups and entrepreneurial ventures initiated by faculty, residents, or students to encourage innovation and commercialization of research.

9. **Funding Digital Resources and Subscriptions** to scientific journals, databases, and other digital resources to provide comprehensive access to the latest research and academic materials.

10. **Student Research Fellowships** for students to engage in full-time research projects during their academic breaks, providing stipends and resources to support their work.

11. **Facilitate Multidisciplinary Research Initiatives** that brings together experts from various fields (such as engineering, management, legal, etc.) to address complex healthcare challenges and foster innovative solutions.

12. **Awards and Recognition Programs** to honor outstanding research contributions, teaching excellence, and innovative projects by faculty, residents, and students.

13. **Data Management and Biostatistics Support** to assist researchers in the design, analysis, and interpretation of their research data.

14. **Visiting Scholar Programs to invite** renowned scholars and researchers to the institution for short-term visits to share their expertise, collaborate on research projects, and deliver lectures or seminars.

3.4 Facility upkeep, beautification and expansion including environmental sustainability (10% ± 5%)

1. **Procurement, operationalization maintenance of electric vehicles**

2. **Street lighting, signages and digital display boards.**
3. **Energy-Efficient Infrastructure** such as LED lighting, smart building technologies to reduce energy consumption and operational costs.
4. **Renewable Energy Sources** as solar panels to generate clean energy for the hospital and reduce reliance on non-renewable energy sources.
5. **Water Conservation Measures** such as rainwater harvesting systems, low- flow faucets and toilets, and greywater recycling systems to reduce water consumption and promote sustainability.
6. **Green Building Certifications:** such as GRIHA to ensure that new constructions and renovations meet high environmental and sustainability standards.
7. **Use of Eco-Friendly Materials** to reduce the environmental footprint of the hospital.
8. **Indoor Air Quality Improvement through indoor plants, air purifiers etc.**
9. **Art and Aesthetic Enhancement** to create a visually pleasing and uplifting environment for patients, visitors, and staff.
10. **Green Roofs:** Creating green roofs on hospital buildings to provide insulation and create additional green spaces
11. **Ensuring Noise Pollution Reduction** through soundproofing materials, quiet zones etc.
12. **Environmental Education Programs** for staff, patients, and visitors to raise awareness about sustainability practices
13. **Green Spaces for Outdoor Therapy** meditation, and relaxation to support the mental and emotional well-being of patients.
14. **Bicycle and Pedestrian Infrastructure** including bike racks, walking paths, and pedestrian-friendly signage to encourage active transportation.
15. **Digital Transformation:** Investing in digital transformation initiatives such as electronic medical records (EMRs), telemedicine, and paperless processes to reduce paper waste and improve operational efficiency.
16. The Institute will ensure that there is no duplication of activities with the funds released under Swachhata Action Plan.

4. MODE OF IMPLEMENTATION

i. The internal revenue will be utilized by the Institute in strict compliance of General Financial Rules, Manual for Procurement of Goods, Guidelines on Make in India and other Instructions issued by the Govt of India from time to time.
ii. The Utilization of the funds will be subject to CAG Audit.

iii. The procurement of goods and services will be undertaken through the GEM (Government E Market) and CPP Portal in accordance with the rules in place on the subject.

iv. In the beginning of every financial year each Institute will prepare the Action Plan for utilization of internal revenue and present the same before the SFC for approval along with the regular Budget Proposal for release of grant in aid.

v. GB/ IB should be kept informed about the utilization of funds .

vi. The Action plan will include activities proposed for patient welfare, employee welfare, research, etc and the funds to be utilized for the same.

vii. Since there is a wide variation in the quantum of internal funds available with the Institutes as some are old and most are relatively new, a limit of how much fund can be utilized in one year may be set with the approval of the SFC. This will enable effective planning and utilizations of internal revenue.

viii. A minimum corpus of fund should be maintained at all time.The institutes may set this limit with the approval of their SFC.

ix. The details of expenditure made in the previous FY along with interest accrued to be presented to the SFC for ratification.

vii. The Institutes should ensure that the expenditure from Internal Revenue is made only on those items which are not covered under Grant-in-Aid. There should not be any duplication.

viii. The Delegation of Financial Powers to the Executive Director of the Institute will be applicable for utilization of the Internal Revenue. The usual mechanism of incurring expenditure out of grant in aid will be followed for utilizing the internal revenue. Therefore the expenditure should be incurred with the concurrence of the Financial Advisor of the institute.

Z-28016/35/2024-PMSSY-IV(8285627)
Government of India
Ministry of Health & Family Welfare
(PMSSY-IV Section)
Room No. 745-A, Nirman Bhawan, New Delhi
Dated the 14-10-2024

Office Order

Subject: Circulation of proposed guidelines for the use of Internal Resources in all new AIIMS/ INIs/ Institutes/ Hospitals of the Ministry - seeking comments/ suggestions. – reg.

This Ministry vide Office Order dated 22.4.2024, constituted a committee to examine the subject of use of Internal Resources for Financial Management with the objective to lay down Guidelines for the use of Internal Revenue generated by the Institutes for their judicious utilization for enhancing patient care services, promotion of research and innovation and employee and student welfare etc.

2. The committee has submitted its report. The report was examined by this Division in consultation with Internal Finance Division (IFD), MoHFW. The Guidelines emerging out of such examination, are enclosed herewith.

3. **As advised by Secretary Health all AIIMS/ INIs/ Institutes/ Hospitals of the Ministry, all Divisional Heads and IFD are requested to examine the guidelines and share the comments/ suggestions to the Ministry at the earliest latest by 28th Oct 2024 to enable this Division to proceed ahead in the matter .**

Signed by
Arun Kumar Biswas
Date: 14-10-2024 19:05:38
(Arun Kumar Biswas)
Under Secretary to the Govt. of India
Tel:011-23061343

Encl(1): Report/ guidelines for the use of Internal Resources in all new AIIMS/ INIs/ Institutes/ Hospitals of the Ministry

To

i. All Additional Secretaries/ Joint Secretaries, MoHFW – with a request to

circulate the proposed Guidelines to all the Institutes/ Hospitals/ Autonomous Bodies under their administrative control.

ii. Director General of Health Services, MoHFW, GoI
iii. AS&FA, MoHFW

Copy to :

i. Director, AIIMS New Delhi
ii. Director, PGIMER, Chandigarh,
iii. Director, JIPMER, Puducherry
iv. Director, NIMHANS, Bengaluru
v. The Directors/ Executive Directors of new AIIMS under PMSSY
vi. The Directors of Central Government Hospitals in Delhi/ North East Hospitals

Copy for information to :

i. PSO to Secretary(HFW)
ii. PPS to Joint Secretary (PMSSY)
iii. PS to Joint Director (PMSSY-IV)

Gmail

pmssysection iv <pmssysectioniv@gmail.com>

Circulation of proposed guidelines for the use of Internal Resources in all new AIIMS/ INIs/ Institutes/ Hospitals of the Ministry - seeking comments/ suggestions. – reg.

1 message

pmssysection iv <pmssysectioniv@gmail.com> Tue, Oct 15, 2024 at 12:36 PM
To: Asfa-mhfw@nic.in, j_mishra@gov.in, asfr-mohfw@gov.in, Roli Singh <roli.singh@ias.nic.in>, ash-mohfw@nic.in, Zhimomiv@ias.nic.in, Dgoffice@naco.gov.in, lschangsan@nic.in, asmd-mohfw@nic.in, jstraining-mohfw@gov.in, Pushpendra.r@nic.in, Vandana.jain@nic.in, Robert.elangbam@gov.in, Sinha.vijay@nic.in, Ea-mohfw@nic.in, kk.tripathy@nic.in, r.wadhawan15@nic.in, jsrch-mohfw@gov.in, cca-mohfw@nic.in, anoopk.puri@nic.in, Ddgtb@rntcp.org, pradeep.khasnobis@gov.in, js-pmssy-mohfw@gov.in, js-publichealth@gov.in, Ankita.edu@nic.in, dghs@nic.in
Cc: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, edaiimsrbl@gmail.com, rajwanshiarvind@hotmail.com, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, "Prof. Dr. D.K. Singh, Director" <director@aiimsbathinda.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, shakti810505@gmail.com, cdskatoch@gmail.com, Executive Director AIIMS Rajkot <ed.aiimsrajkot@gmail.com>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, madhabananda@gmail.com, sachimohanty@rediffmail.in, Dr Vivek Lal <dpgi@pgimer.edu.in>, director@jipmer.ac.in, director@aiims.gov.in, Director Neigrihms <director-neigrihms@gov.in>, nalinaiims.mehta@gmail.com, eigasunil@gmail.com, director@ripans.ac.in, MS OFFICE SJH <msoffice@vmmc-sjh.nic.in>, "Dr. Sunita Sharma" <director-lhmc@gov.in>, minakshi Bhardwaj <med.sup@rmlh.nic.in>, secyhfw@nic.in, Praveen.batra@gov.in, "Cc:" <dinesh.kumar14@nic.in>, ":" <ak.biswas57@nic.in>, sankar.garg@gov.in, Amit Batra <amit.batra@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officials of PMSSY-IV Section at - dinesh.kumar14@nic.in; ak.biswas57@nic.in; sankar.garg@gov.in; amit.batra@gov.in

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

2 attachments

Office Order 2.pdf
81K

encl.docx
28K

Proposed guidelines for the use of Internal Resources in all new AIIMS/ INIs/ Institutes/ Hospitals of the Ministry

The General Financial Rules lay down the principles for setting up of Autonomous Organizations and their fund management. The Guidelines will be operational within the ambit of the GFRs.

As per Rule 229 (iv) states that All autonomous organizations, new or already in existence should be encouraged to maximize generation of internal resources and eventually attain self-sufficiency.

Rule 229 (v) provides that the Ministry or Department may consider creating a Corpus Fund for an Autonomous Body only with prior concurrence of Ministry of Finance if the corpus is created out of budgetary allocation. If the corpus is created out of internal accruals of the body, approval of the administrative Ministry must be obtained.

2. The major source of Internal Revenue Generation include :

Heads	Description
Hospital	a. User Fees: Patient Registration, Day-Care & Indoor Admission Fees, Bed Charges (General Ward) & Room Rent (Private Ward), OT Charges for procedures & surgeries, Pathological & Radiological investigations. b. Service charges: Vaccination, Mortuary, Embalming, etc. c. Pharmacy Charges: Implants, vaccines, Drugs, etc. d. Insurance claims: TPA, CGHS, etc. e. AB-PMJAY reimbursements.
Academic Fees	a. Admission fees from students/ trainees/fellowship programmes. b. Unspent balance of various workshops/ training programmes. c. Externships. d. Auditorium charges.

Research Grant	a. Collaborations with external agencies to create new commercialized products, like rapid diagnostic tests etc. b. Patent charges. c. Overhead charges from External Research Projects
Examination Fees	a. Examination fees from applicants for recruitments. b. National Exams like NEET, NORCET etc.
Any Other	CSR/ Philanthropy and Donation Any Other a. Start-ups in the Institutes. b. Penalty charges from defaulter firms/vendors c. Penalty from students & staff d. Sale of scrap material. e. Rental charges (shops, ATMs, parking, canteen etc.). f. Collection on account of shortfall in notice period of employees resigning. g. Electricity & water charges from various vendors and contractors (Engineering works). h. Interest earned from internal receipts savings bank account & Fixed Deposits & Security Deposits of tenders. i. Income from Guest house receipts.

3. In accordance with the recommendation of the committee set up the Ministry on the above subject the internal revenue of the Institute can be broadly utilized for the following purpose and in the proportion indicated:

3.1 Patient Welfare (50% ± 5%)

1. **To support emergency health** care needs within the institution.

2. **To undertake Community Outreach activities for** extending healthcare services to the broader community.

3. **Patient Welfare Activities designed to improve the well-being and comfort of patients and their attendants by** development of facilities such as Vishram Sadans (rest houses), waiting halls, cafeterias, access to clean drinking water, play areas and libraries for children etc.

4. **Patient Navigation Services** to guide patients and their families through the complex healthcare system through intra-hospital navigation app /engaging volunteers etc.

5. **Quality Improvement Initiatives including** Accreditation programs such as NABH (National Accreditation Board for Hospitals & Healthcare Providers), NQAS (National Quality Assurance Standards), and NABL (National Accreditation Board for Testing and Calibration Laboratories)

6. **Innovation and Pilots:** for advancing healthcare practices and exploring new approaches to patient care. These initiatives may include testing new technologies, treatment protocols, and service delivery models on a small scale before broader implementation.

7. **Health Education and Awareness Programs** for patients and their families to enhance their understanding of health conditions, treatment options, and preventive measures.

8. **Holistic Health Support:** Providing mental health services, counselling complementary therapies such as yoga, meditation, acupuncture, and music therapy to support traditional medical treatments and improve patient well- being.

9. **Support for Chronic Disease Management for diseases** such as diabetes, hypertension, heart disease, through regular medication management, and lifestyle coaching.

10. **Rehabilitation Services:** such as physical therapy, occupational therapy, and speech therapy to aid in the recovery and improve the quality of life for patients with disabilities or those recovering from surgeries and illnesses.

11. **Palliative and End-of-Life Care** for patients with life-limiting illnesses, focusing on pain relief, emotional support etc.

12. **Establishing mechanisms for Feedback and Patient Advocacy** to ensure that the patient's voice is heard, and their rights are protected within the healthcare system.

13. **Volunteer Programs** where community members can contribute their time and skills to support various patient welfare activities

14. **Promotion of Digital Health through use of** ABDM , mobile apps, telemedicine, patient portals and other platforms /apps

15. **Cultural and Recreational Activities** within the hospital to provide emotional relief and improve the morale of patients.

3.2 Employee Welfare **(20% ± 5%)**

1. **Promoting Team Building and Enhancing Motivation through workshops, trips etc. Investing in tools and technologies that facilitate better collaboration and communication among team members.**

2. **Recreational Activities like Annual Sports/Cultural Programs** for fostering a positive and inclusive workplace culture, encouraging physical fitness, fostering creativity and talent and improving work life balance.

3. **Faculty and Student Exchange Programme for Networking and Learning Best Practices.**

4. **Professional Development Programs** including workshops, seminars, online courses, and certification programs to enhance the skills and knowledge of employees.
5. **Health and Wellness Programs** to promote the physical and mental well- being of employees.
6. **Employee Recognition and Reward Programs** to acknowledge and appreciate the hard work and achievements of employees.
7. **Counselling and Support Services to help** employees to deal effectively with personal or work-related issues. Implementing programs to identify, prevent, and manage burnout among healthcare workers,
8. **Ensuring Safety and Ergonomics** by conducting regular safety audits, providing ergonomic workstations, offering training on workplace safety practices etc.
9. **Team Collaboration Tools:** such as project management software, instant messaging platforms, and video conferencing tools.
10. **Support for Shift Workers:** Providing specialized support for employees working in shifts, such as sleep management programs, healthy meal options available at all hours, and flexible scheduling to reduce fatigue.
11. **Crisis Management Training:** Providing training on crisis management, including handling medical emergencies, natural disasters etc.
12. **Wellness Rooms and Rest Areas:** Creating dedicated wellness rooms and rest areas within the hospital where staff can take breaks, relax, and recharge during their shifts.
13. No Allowances to be paid to employees out of the Internal Revenue

3.3 Academic and Research Welfare (20% ± 5%)

1. **Scholarships** to students for extra trainings courses andresearch.

2. **Academic trips and Faculty Exchange programme** to other institutes to understand best practices, to promote cross-pollination of ideas, collaborative research, and exposure to diverse teaching and research practices.

3. Mess facility for economically weak students or any other help required as deemed fit by Director.

4. **Conference Sponsorships for** national and international conferences for faculty, residents, and students to present their research findings.

5. **Professional Development Workshops** on research methodologies, research ethics, regulatory compliance, scientific writing, and data analysis to enhance the research skills of faculty and students.

6. **Facilitate Collaboration with Industry and Academia** to promote joint research projects, internships, and academic exchange programs.

7. **Publication Support** for the publication of research findings in reputed journals.

8. **Seed Funding for** healthcare-related startups and entrepreneurial ventures initiated by faculty, residents, or students to encourage innovation and commercialization of research.

9. **Funding Digital Resources and Subscriptions** to scientific journals, databases, and other digital resources to provide comprehensive access to the latest research and academic materials.

10. **Student Research Fellowships** for students to engage in full-time research projects during their academic breaks, providing stipends and resources to support their work.

11. **Facilitate Multidisciplinary Research Initiatives** that brings together experts from various fields (such as engineering, management, legal, etc.) to address complex healthcare challenges and foster innovative solutions.

12. **Awards and Recognition Programs** to honor outstanding research contributions, teaching excellence, and innovative projects by faculty, residents, and students.

13. **Data Management and Biostatistics Support** to assist researchers in the design, analysis, and interpretation of their research data.

14. **Visiting Scholar Programs to invite** renowned scholars and researchers to the institution for short-term visits to share their expertise, collaborate on research projects, and deliver lectures or seminars.

3.4 Facility upkeep, beautification and expansion including environmental sustainability (10% ± 5%)

1. **Procurement, operationalization maintenance of electric vehicles**

2. **Street lighting, signages and digital display boards**.
3. **Energy-Efficient Infrastructure** such as LED lighting, smart building technologies to reduce energy consumption and operational costs.
4. **Renewable Energy Sources** as solar panels to generate clean energy for the hospital and reduce reliance on non-renewable energy sources.
5. **Water Conservation Measures** such as rainwater harvesting systems, low- flow faucets and toilets, and greywater recycling systems to reduce water consumption and promote sustainability.
6. **Green Building Certifications:** such as GRIHA to ensure that new constructions and renovations meet high environmental and sustainability standards.
7. **Use of Eco-Friendly Materials** to reduce the environmental footprint of the hospital.
8. **Indoor Air Quality Improvement through indoor plants, air purifiers etc.**
9. **Art and Aesthetic Enhancement** to create a visually pleasing and uplifting environment for patients, visitors, and staff.
10. **Green Roofs:** Creating green roofs on hospital buildings to provide insulation and create additional green spaces
11. **Ensuring Noise Pollution Reduction** through soundproofing materials, quiet zones etc.
12. **Environmental Education Programs** for staff, patients, and visitors to raise awareness about sustainability practices
13. **Green Spaces for Outdoor Therapy** meditation, and relaxation to support the mental and emotional well-being of patients.
14. **Bicycle and Pedestrian Infrastructure** including bike racks, walking paths, and pedestrian-friendly signage to encourage active transportation.
15. **Digital Transformation:** Investing in digital transformation initiatives such as electronic medical records (EMRs), telemedicine, and paperless processes to reduce paper waste and improve operational efficiency.
16. The Institute will ensure that there is no duplication of activities with the funds released under Swachhata Action Plan.

4. MODE OF IMPLEMENTATION

i. The internal revenue will be utilized by the Institute in strict compliance of General Financial Rules, Manual for Procurement of Goods, Guidelines on Make in India and other Instructions issued by the Govt of India from time to time.
ii. The Utilization of the funds will be subject to CAG Audit.

iii. The procurement of goods and services will be undertaken through the GEM (Government E Market) and CPP Portal in accordance with the rules in place on the subject.

iv. In the beginning of every financial year each Institute will prepare the Action Plan for utilization of internal revenue and present the same before the SFC for approval along with the regular Budget Proposal for release of grant in aid.

v. GB/ IB should be kept informed about the utilization of funds .

vi. The Action plan will include activities proposed for patient welfare, employee welfare, research, etc and the funds to be utilized for the same.

vii. Since there is a wide variation in the quantum of internal funds available with the Institutes as some are old and most are relatively new, a limit of how much fund can be utilized in one year may be set with the approval of the SFC. This will enable effective planning and utilizations of internal revenue.

viii. A minimum corpus of fund should be maintained at all time.The institutes may set this limit with the approval of their SFC.

ix. The details of expenditure made in the previous FY along with interest accrued to be presented to the SFC for ratification.

vii. The Institutes should ensure that the expenditure from Internal Revenue is made only on those items which are not covered under Grant-in-Aid. There should not be any duplication.

viii. The Delegation of Financial Powers to the Executive Director of the Institute will be applicable for utilization of the Internal Revenue. The usual mechanism of incurring expenditure out of grant in aid will be followed for utilizing the internal revenue. Therefore the expenditure should be incurred with the concurrence of the Financial Advisor of the institute.

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Procedure lor reporting, reviewing and accepting of Annual Performance Assessment Reports (APARS) of Financial Advisors in new AIIMS -reg.

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, Dec 18, 2025 at 10:54 AM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **pmssysection iv** <pmssysectioniv@gmail.com>
Date: Thu, Feb 20, 2025 at 10:56 AM
Subject: Procedure lor reporting, reviewing and accepting of Annual Performance Assessment Reports (APARS) of Financial Advisors in new AIIMS -reg.
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, Executive Director Raebareli <edaiimsrbl@gmail.com>, <rajwanshiarvind@hotmail.com>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, <madhabananda@gmail.com>, <sachimohanty@rediffmail.in>
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, <dda@aiimsrbl.edu.in>, Dr. PRADIP KUMAR <kpradip10@gmail.com>, <dda@aiimskalyani.edu.in>, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, Rajeev Sen Roy <rajeevsenroy30@gmail.com>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, <dda@aiimsbilaspur.edu.in>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, Administrative Officer <ao.aiimsmadurai@gmail.com>, T Ngamlien <t.ngamlien@icg.gov.in>, Mukesh Kumar <mac.prasad@gmail.com>, <ddaaiimsawantipora1@gmail.com>, Dy Director Administration AIIMS, Raebareli <ddaaiimsrbl@gmail.com>, <fa@aiimsrishikesh.edu.in>, <acctsofficeraiimsjammu@gmail.com>, <jgoswami@aiimsjammu.edu.in>, Apurva Chandra <secyhfw@nic.in>, Praveen Batra <Praveen.batra@gov.in>, Cc: <Dinesh.kumar14@nic.in>, : <Ak.biswas57@nic.in>, Vaishali Vinayak <vaishali.vinayak@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officials of

PMSSY-IV Section at - dinesh.kumar14@nic.in; ak.biswas57@nic.in; vaishali.vinayak@gov.in;

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

Letter (27).pdf
573K

No.: Z-11019/11/2025-PMSSY-IV
Government of India
Ministry of Health and Family Welfare
***

Room No:201-D, Nirman Bhawan, New Delhi
Dated 19-02-2025

To

All Executive Directors, of New AIIMS under PMSSY

Subject: Procedure for reporting, reviewing and accepting ofAnnual Performance Assessment Reports (APARs) of Financial Advisors in new AIIMS -reg.

Sir,

Please refer to this Ministry's letter No.Z.28016/6/2013-SSH, dated 09.08.2016 (copy enclosed) regarding procedure for reporting, reviewing and accepting of Annual Confidential Reports of the Project Cell Posts.

2. In this connection, I am directed to convey the approval of the competent authority regarding **revised** reporting channel for submission of APARs in respect of **Financial Advisors (FAs) of all new AIIMS under PMSSY**:

Post	Reporting Officer	Reviewing Officer	Accepting Authority
Financial Advisor	Executive Director, AIIMS	Joint Secretary (PMSSY)	Additional Secretary/ Secretary (HFW) as the case may be.

3. It is also advised that the officers should get their APARs reported and reviewed from their Reporting and Reviewing Officers as per stipulated timelines.The Institutes should also maintain a record of the APARs of the officers for future reference .

Yours faithfully,

Digitally signed by Dinesh Kumar
Date: 19-02-2025 18:25:48

(Dinesh Kumar)
Director, MoHFW, GoI
Tele 011-23061730

Copy to:

(i) Financial Advisors of All new AIIMS under PMSSY

(ii) All Dy. Directors (Admin), of New AIIMS under PMSSY.

Copy also to for information

(i) PSO to Secretary (HFW)

(ii) PS to JS (PMSSY)

30

No. Z. 28016/6/2013-SSH
Government of India
Ministry of Health & Family Welfare
PMSSY Division

Nirman Bhawan, New Delhi- 110108
Dated : 9th August 2016

To,

The Director, AIIMS Bhopal
The Director, AIIMS Bhubaneswar
The Director, AIIMS Jodhpur
The Director, AIIMS Patna
The Director, AIIMS Raipur
The Director, AIIMS Rishikesh

Subject : Procedure for reporting , reviewing and accepting of Annual Confidential Reports of the Project Cell posts in six new AIIMS

Sir,

The Competent Authority has approved the following reporting channel for the Project Cell posts of the six new AIIMS

Post	Reporting officer	Reviewing officer	Accepting Authority
Director	Secretary (HFW)	President , AIIMS	President , AIIMS
Deputy Director (Admn.)	Director, AIIMS	Joint Secretary (PMSSY)	Additional Secretary (PMSSY)
Financial Advisor	Director , AIIMS	Joint Secretary (PMSSY)	Additional Secretary & Financial Advisor (MoHFW)
Medical Superintendent	Director , AIIMS	Additional Secretary (PMSSY)	Secretary (HFW)
Superintending Engineer	Director , AIIMS	Joint Secretary (PMSSY)	Additional Secretary (PMSSY)

2 It is also requested to the Officers that they may get their ACRs reported and reviewed directly from their Reporting and Reviewing Officers. A record of the ACRs should also be maintained by the respective AIIMS.

Yours faithfully,

(P. A Mini)
Director
Tel: 011- 23061288

Copy to:
PS to HFM /PS to Secretary (HFW)/ PPS to AS (Health)/ PPS to AS& FA/ PPS to JS (PMSSY)

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Guidelines concerning identification of posts for persons with benchmark disabilities and their reservation in Central Government Establishments for effective implementation of the RPwD Act, 2016 - reg.

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, Dec 18, 2025 at 10:54 AM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **pmssysection iv** <pmssysectioniv@gmail.com>
Date: Mon, Feb 24, 2025 at 2:45 PM
Subject: Guidelines concerning identification of posts for persons with benchmark disabilities and their reservation in Central Government Establishments for effective implementation of the RPwD Act, 2016 - reg.
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, Executive Director Raebareli <edaiimsrbl@gmail.com>, <rajwanshiarvind@hotmail.com>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, <madhabananda@gmail.com>, <sachimohanty@rediffmail.in>
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, <dda@aiimsrbl.edu.in>, Dr. PRADIP KUMAR <kpradip10@gmail.com>, <dda@aiimskalyani.edu.in>, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, Rajeev Sen Roy <rajeevsenroy30@gmail.com>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, <dda@aiimsbilaspur.edu.in>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, Administrative Officer <ao.aiimsmadurai@gmail.com>, T Ngamlien <t.ngamlien@icg.gov.in>, Mukesh Kumar <mac.prasad@gmail.com>, <ddaaiimsawantipora1@gmail.com>, Dy Director Administration AIIMS, Raebareli <ddaaiimsrbl@gmail.com>, Cc: <Dinesh.kumar14@nic.in>, : <Ak.biswas57@nic.in>, <dev.gothal@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officials of

PMSSY-IV Section at - dinesh.kumar14@nic.in; ak.biswas57@nic.in; dev.gothal@gov.in;

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

---

2 attachments

Letter (108).pdf
92K

Encl (35).pdf
5084K

No. Z-28015/04/2025-PMSSY-IV
Government of India
Ministry of Health and Family Welfare
(PMSSY-IV Section)
*****

745 A, 7th Floor, Nirman Bhawan, New Delhi
Dated 20-02-2025

To,

The Executive Directors, all new AIIMS.

Subject: Guidelines concerning identification of posts for persons with benchmark disabilities and their reservation in Central Government Establishments for effective implementation of the RPwD Act, 2016 - reg.

Sir,

I am directed to enclose herewith a copy of OM No. CA.14020/04/2024-W&PG dated 14.01.2025 along with Department of Empowerment of Persons with Disabilities (DEPwD)'s OM No. 41-01/2024-DD-III (CN: 37325) dated 08.11.2024, received from W&PG Section, MoHFW on the above mentioned subject for compliance of the guidelines issued by DEPwD.

Yours faithfully,

Digitally signed by
ARUN KUMAR BISWAS
Date: 20-02-2025
17:50:11

(Arun Kumar Biswas)
Under Secretary to the Govt. of India
Tele: 011-23061343

Encl: As above

Copy to :

i. Deputy Director (Admn.), all new AIIMS

F.No. A.14020/04/2024-W&PG
Government of India
Ministry of Health & Family Welfare
(Welfare & PG Section)

Nirman Bhawan, New Delhi
Dated 14-01-2025

OFFICE MEMORANDUM

Subject: Guidelines concerning identification of posts for persons with benchmark disabilities and their reservation in Central Government Establishments for effective implementation of the RPwD Act, 2016.

The undersigned is directed to forward herewith a copy of Office Memorandum No. 41-1/2024-DD-III (CN: 37325) dated 08.11.2024 (copy enclosed) issued by the Department of Empowerment of Persons with Disabilities (Divyangjan), Ministry of Social Justice & Empowerment on the subject cited above.

2. All Divisions are requested to issue instructions to all Central Government Hospitals/ Attached Offices/ Subordinate Offices/ Autonomous Bodies under their administrative control to ensure compliance with the guidelines, including formation of a Committee for identification of posts suitable for persons with benchmark disabilities (PwDs).

Encl: As above.

Digitally signed by
ANANT KUMAR
Date: 14-01-2025
11:20:28

(Anant Kumar)
Under Secretary to the Government of India
Tel. No. 011-23061640

To

1) All Additional Secretaries/ DG(Stats)/ Sr. EA(IK)/ Joint Secretaries/ JS(GM) of Dte.GHS / Advisor (RW)/ EA (KKT)/ CCA/ Director (CGHS)

2) All Directors/ Deputy Secretaries/ equivalent officers.

Copy to (for information):

PSO to Secretary (HFW)

सं./ No. 41-01/2024-DD-III (CN: 37325)
भारत सरकार / Government of India
सामाजिक न्याय और अधिकारिता मंत्रालय/Ministry of Social Justice & Empowerment
दिव्यांगजन सशक्तिकरण विभाग
Department of Empowerment of Persons with Disabilities (Divyangjan)

पाँचवा तल, पंडित दीनदयाल अंत्योदय भवन
5th Floor, Pt. Deendayal Antyodaya Bhawan
सी जी ओ कॉप्लेक्स, लोधी रोड, नई दिल्ली -110003
CGO Complex, Lodhi Road, New Delhi-110003
दिनांक / Dated: 08.11.2024

कार्यालय ज्ञापन / OFFICE MEMORANDUM

Subject: **Guidelines concerning identification of posts for persons with benchmark disabilities and their reservation in the Central Government Establishments for the effective implementation of the Rights of Persons with Disabilities Act, 2016 (RPwDAct, 2016) in pursuance of orders of the Hon'ble High Court of Delhi in W.P. (C) No. 17460/2022 and W.P. (C) No. 665/2023 in the matter of Kendriya Vidyalaya Sangathan (KVS) and Ors vs Union of India and ors**

The undersigned is directed to refer to the order dated 01.11.2023 passed by the Hon'ble High Court of Delhi in W.P. (C) No. 17460/2022 and W.P. (C) No. 665/2023 in the matter of Kendriya Vidyalaya Sangathan (KVS) and Ors vs Union of India and ors and to say the following observations were made in the said order:

i. That KVS assumed a power which was never vested in it by constituting its own committee to identify posts suitable for persons with benchmark disabilities (PwBDs),

ii. That there is a mismatch in the understanding of different Departments regarding the mandate under the RPwD Act, and

iii. That the concerned Secretary of the Department i.e. DEPwD, is directed to issue suitable guidelines for the implementation of reservation policy by all the Departments in a uniform manner.

2. Based on the directions of Hon'ble High Court of Delhi in above stated matter, the Central Government hereby lays down the **"Guidelines for identification of posts for persons with benchmark disabilities and their reservation in Central Government Establishments"** as under:

File No. A-14020/04/2024-W&PG (Computer No. 8307931)
File No. Z-28015/04/2025-PMSSY-IV (Computer No. 8313935)
Generated from eOffice by SARITA, EA(S)-PMSSY, DEO, DOHFW DEPARTMENT on 24/02/2025 02:42 pm

2.1: Chapter-I (Identification of Posts)

i. Section 33 of the RPwD Act, 2016 deals with identification of posts for PwDs for the purpose of reservation. It mandates the Government to:

(a) identify posts in the establishment which can be held by respective category of persons with benchmark disabilities (i.e where disability is 40% and above) in respect of the vacancies reserved in accordance with the provisions of Section 34 of the RPwD Act, 2016,
(b) constitute an expert committee with representation of persons with benchmark disabilities for identification of such posts, and
(c) undertake periodic review of the identified posts at an interval not exceeding three years.

ii. There was a similar provision in the erstwhile legislation namely the Persons with Disabilities (Equal Opportunities, Protection of Rights and Full Participation) Act, 1995 to identify posts suitable for PwDs. A notification on the subject was issued by DEPwD on 29.7.2013.

iii. After the enactment of RPwD Act, 2016, since the process of identification of posts suitable for persons with benchmark disabilities was taking time, this Department had requested all the Central Ministries/Departments to identify posts for persons with benchmark disabilities at their own level so that vacancies are filled up as per the RPwD Act, 2016 in time.

iv. In the meanwhile, the Department had also constituted an expert committee on 19.11.2015 for identification of suitable posts for persons with benchmark disabilities with representatives from DEPwD; D/o Personnel and Training; M/o Health and Family Welfare; D/o Public Enterprises; Ministry/Department concerned i.r.o. which identification of jobs and related matters are to be reviewed; Director General of Employment and Training; HoD, PMR, Safdarjung Hospital, National Institutes on each disability and NGOs. This expert committee further constituted five Sub- Committees for i. locomotor disability, ii. hearing impaired, iii. visually impaired, iv. autism, specific learning disability, mental illness and intellectual disabilities and v. multiple disabilities to take care of identification of posts suitable for PwBDs.

v. The gist of the report of Expert Committee i.e. the list of suitable posts to be reserved for PwBDs in Central Ministries, Departments, Public Sector Undertakings and Autonomous Bodies (total 3566 posts) is notified *vide* **notification no. 38-16/2020-DD-III dated 04.01.2021** which is available on the website of the Department i.e. www.depwd.gov.in. As per the said notification, the list of posts being notified is **only indicative** and **not an exhaustive list**. The Central Ministries, Departments, Public Sector Undertakings and Autonomous

File No. A.14020/04/2024-W&PG (Computer No. 8307921)
File No. Z-28015/04/2025-PMSSY-IV (Computer No. 8313935)
Generated from eOffice by SARITA, EA(S)-PMSSY, DEO, DOHFW DEPARTMENT on 24/02/2025 02:42 pm

Bodies may further supplement the list by adding to the list of posts identified for respective category of disability.

vi. Further, in pursuance of the provisions of said Act, **review of identified posts is to be conducted in an interval not exceeding 3 years**. In order to ensure that this review is done timely, following procedure needs to be complied with by all the Central Ministries/Departments:

(a) Every post under the Central Ministry/Department including the posts in public sector enterprises, autonomous organisations and other establishments needs to be considered for determining its suitability for persons with benchmark disabilities and no post should be left out. In case any post is left out, such post will be deemed to be open for all categories of disabilities which are eligible for reservation unless it is exempted by notification of DEPwD.

(b) **Each Central Ministry/Department will constitute a committee consisting of representatives of persons with benchmark disabilities and recommend suitable posts for PwDs to DEPwD for consideration and notification, wherever necessary.** This committee should have at least one representative with benchmark disabilities each from following categories:

- blindness and low vision;
- deaf and hard of hearing;
- locomotor disability including cerebral palsy, leprosy cured, dwarfism, acid attack victims and muscular dystrophy; and
- autism, intellectual disability, specific learning disability and mental illness.

The said Committee is required to look into the suitability of each/all post(s) in their establishments for specified category of disabilities taking into consideration the development in assistive technologies, the principal list of identified posts dated 04.01.2021 and global benchmarks in employment of PwDs. Such Committee is to be constituted at the level of Ministry/ Departments only, and not below that by PSUs/ autonomous bodies etc. and should be headed by Additional/Joint Secretary level officer. In terms of Note 2 of the gist of recommendations contained in DEPwD's notification dated 04.01.2021, the Ministry/Department may add to the list of posts or the sub-category/ category of disability based on the recommendations of the above mentioned Committee under intimation to this Department. However, no post or category or sub category existing in the notification of DEPwD dated 04.01.2021 or any such notification issued on the subject subsequently by the DEPwD can be reduced without obtaining approval of DEPwD.

(c) **DEPwD will constitute a broad-based expert committee** consisting of representatives of concerned Ministries/Departments, persons with benchmark disabilities, Chief Commissioner for Persons with Disabilities, experts and National Institutes. On the basis of recommendation of this Committee, **DEPwD will notify the list of suitable posts** in respect of posts of all Central

File No. A-14020/04/2024-W&PG (Computer No. 8307921)
File No. Z-28015/04/2025-PMSSY-IV (Computer No. 8313935)
Generated from eOffice by SARITA, EA(S)-PMSSY, DEO, DOHFW DEPARTMENT on 24/02/2025 02:42 pm

Ministries/Departments including CPSUs and autonomous bodies functioning under their administrative control on the lines of notification dated 04.01.2021. This review of job mapping exercise (notification no. 38-16/2020-DD-III dated 04.01.2021) is needed as nomenclature/job requirement of some posts might have changed, some new kind of posts may have got added, and also because latest advancement in assistive technologies now enable PwDs to do things which were not possible a few years ago. The exercise will cover all the posts common to more than one Ministry/Department along with posts which are specific to a single Ministry/Department. As indicated earlier in para 2.1 (v), list of posts dated 04.01.2021 is only indicative and not an exhaustive list. Central Ministries, Departments, Public Sector Undertakings and Autonomous Bodies may further supplement the list by adding to the list of posts identified for respective category of disability.

2.2: Chapter-II (Exemption)

i. Second proviso to section 34 (1) of the RPwD Act, 2016 empowers the Government to exempt any government establishment from the provision of this Section. **DEPwD is the competent authority to consider and notify such exemption.**

ii. Since identification of posts is a dynamic process, exemption will also be reviewed from time to time in the light of advancement of technology, availability of new and more efficient assistive devices, increase in capacity of persons with disability etc. **As such, any exemption is valid for a maximum period of 3 years. In case of those establishments in r/o of which exemption has already been granted by DEPwD and the period of 3 years from the date of notification of exemption has elapsed, they may approach DEPwD, within a period of 3 months from the date of issuance of this OM with fresh proposal to review the exemption.**

iii. **It is emphasized that identification exercise should be carried out with due diligence and utmost care so that there is no requirement of seeking exemption during the 3 year window.**

2.3: Chapter-III (Reservation in direct recruitment and promotion)

i. Section 34 of the said Act deals with percentage of reservation in vacancies in Government establishments. As per Allocation of Business Rules, 1961, DEPwD is the nodal Department for overall policy, planning and coordination of programmes for Persons with Disabilities. DoPT issues instructions relating to reservation of vacancies in posts and services under the Central Government based on the policy decisions taken by DEPwD in respect of PwDs. Accordingly,

File No. A.14020/04/2024-W&PG (Computer No. 8307921)
File No. Z-28015/04/2025-PMSSY-IV (Computer No. 8313935)
Generated from eOffice by SARITA, EA(S)-PMSSY, DEO, DOHFW DEPARTMENT on 24/02/2025 02:42 pm

DoPT, *vide* its **O.M. no. 36035/02/20217-Estt (Res) dated 15.01.2018** has issued detailed instructions providing reservation for PwDs in vacancies to be filled by direct recruitment. Further, vide **OM No. 36012/1/2020-Estt (Res.II) dated 17.05.2022**, read with **OM of even no. dated 28.12.2023**, DoPT has issued instructions providing reservation in promotion to PwDs. All the Central Ministries/Departments are requested to bring the above instructions to the notice of all appointing authorities under their control.

ii. It is stated that the 4% reservation for PwBDs is to be extended in terms of Section 34 of the RPwD Act, 2016 as under:

(a)	blindness and low vision	1%
(b)	deaf and hard of hearing	1%
(c)	locomotor disability including cerebral palsy, leprosy cured, dwarfism, acid attack victims and muscular dystrophy;	1%
(d)	autism, intellectual disability, specific learning disability and mental illness;	1%
(e)	multiple disabilities from amongst persons under clauses (a) to (d) including deaf- blindness.	

iii. Where in any recruitment year any vacancy cannot be filled up due to non availability of a suitable person with benchmark disability or for any other sufficient reason, the process of carry forward of vacancy/reservation and *inter se* exchange of reservation is to be carried out in terms of **DoPT's instructions dated 15.01.2018 and 17.05.2022.**

iv. The objective of reservation gets fulfilled only if existing as well as backlog vacancies are filled in time, and also after giving wide publicity for the benefit of persons with disabilities which may also include intimation to the associations of persons with disabilities and placing the information on their official website.

v. At the time of promotion, **Note 4 of DEPwD's notification dated 04.01.2021** on identification of posts may be kept in mind which states that **"If a post is identified in the feeder grade, all the posts in the promotional grade should also stand identified".**

vi. Rajasthan High Court in its judgment in the case of Rekha Meena vs State of Rajasthan 2020 ruled that persons with disability (with disability of 40% or more or even less) cannot be denied appointment on the ground of disability, if they did not claim reservation benefit available to them. In this context, DOPT had issued detailed clarification vide its **OM no. 36035/02/20217-Estt (Res) dated 27.09.2022** relating to reservation of persons with benchmark disabilities as to the concept of own merit. This needs to be followed in letter and spirit.

File No. A-14020/04/2024-W&PG (Computer No. 8307921)
File No. Z-28015/04/2025-PMSSY-IV (Computer No. 8313935)
Generated from eOffice by SARITA, EA(S)-PMSSY, DEO, DOHFW DEPARTMENT on 24/02/2025 02:42 pm

3. These guidelines are formulated in consultation with Chief Commissioner for PwDs, DOPT and Ministry of Law and Justice.

4. These guidelines are effective from the date of issuance.

5. This OM is being issued in supersession of all earlier instructions issued by DEPwD on the subject except the **notification no. 38-16/2020-DD-III dated 04.01.2021 and 30-12/2020 DD-III dated 24.08.2022**.

6. This issues with the approval of Hon'ble Union Minister for Social Justice and Empowerment.

Bhjee 08.11.2024.

(देबाला भट्टाचार्य/Debala Bhattacharjee)
अवर सचिव, भारत सरकार/ Under Secretary to the Govt of India
दूरभाष/Tel: 2436-6027

To,

The Secretaries of all Central Ministries/Departments
(As per standard list)

File No. A.14020/04/2024-W&PG (Computer No. 8307921)
File No. Z-28015/04/2025-PMSSY-IV (Computer No. 8313935)
Generated from eOffice by SARITA, EA(S)-PMSSY, DEO, DOHFW DEPARTMENT on 24/02/2025 02:42 pm

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Procurement and Placement of BHISM Cube at Identified Central Government Hospitals/Institutes-reg

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, Dec 18, 2025 at 10:53 AM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **VIKASH KUMAR GUPTA** <vikas.kumar76@gov.in>
Date: Mon, Mar 3, 2025 at 2:38 PM
Subject: Procurement and Placement of BHISM Cube at Identified Central Government Hospitals/Institutes-reg
To: dda <dda@aiimsmangalagiri.edu.in>, dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsrishikesh.edu.in>, Dy. Director Administration <dda@aiimsraipur.edu.in>, dda <dda@aiimspatna.org>, dda <dda@aiimsbhubaneswar.edu.in>, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, ddaaiimsjodhpur <dda.aiimsjodhpur@gmail.com>, dda <dda@aiimsbibinagar.edu.in>, dda <dda@aiimsbilaspur.edu.in>, dda <dda@aiimsdeoghar.edu.in>, ddaaiimsrbl <ddaaiimsrbl@gmail.com>, dda <dda@aiimsgorakhpur.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, Director JIPMER <director@jipmer.edu.in>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, Pgimer12 <pgimer12@yahoo.com>, dda <dda@aiimsbathinda.edu.in>, dps <dps@hllhites.com>, ceo <ceo@hllhites.com>, Pradeepkhasnobis <Pradeep.khasnobis@gov.in>, Dharm Bir Kumar SIngh <dharmbk.singh@nic.in>, director-neigrihms@gov.in <nalinaiims.mehta@gmail.com>, director <director@aiims.gov.in>, director <director@jipmer.ac.in>, unnism <unnism@lifecarehll.com>, vishalagarwal <vishalagarwal@lifecarehll.com>
Cc: PUNYA SALILA SRIVASTAVA <secyhfw@nic.in>, ANKITA MISHRA BUNDELA <js-pmssy-mohfw@gov.in>, Shri Raj Kumar Deputy Secretary <raj.kumar28@nic.in>, Ravi Kumar <ravi.kumar89@gov.in>, Mayukh Ranjan Paul <mayukh.paul88@gov.in>

Sir/Ma'am

Please find attachment on the subject cited above for necessary action.

Thanks & Regards
Vikash Kumar Gupta, Central Secretariat Service (CSS)
Assistant Section Officer
PMSSY-I
Ministry of Health & Family Welfare
Govt. of India



Please consider your environmental responsibility. Before printing this e-mail message, ask yourself whether you really need a hard copy.

---

2 attachments

BHISM Cube.pdf
85K

OM BHISM Cube.pdf
6953K

F.No. Z-28016/125/2024-PMSSY-V (8283121)
Government of India
Ministry of Health & Family Welfare
(PMSSY-I Section)

Nirman Bhawan, New Delhi
Dated: 03-03-2025

To

The Director/Executive Directior of AIIMS/INIs
(as per list attached)

Subject:- Procurement and Placement of BHISM Cube at Identified Central Government Hospitals/Institutes-reg.

Sir/Ma'am,

I am directed to forward the Disaster Management Cell (DM Cell)'s OM No. D-32020/1/2022-DM Cell/Mobile Hospital (Part) dated 27.02.2025 regarding installation of BHISM Cubes in various Institutes of the Ministry by HLL Life Care , Standard Operating Procedure for logistics and the role and responsibilities of the Institutes for their their use for necessary compliance under intimation to the Ministry .

Encl:- As above.

Yours faithfully

Digitally signed by
Raj Kumar
(Raj Kumar)
Date: 03-03-2025
09:45:39

Dy. Secretary to the Government of India
Tel-011-23063178

Copy to:-

1. Dr. Pradeep Khasnobis, DDG, DM Cell, MoH&FW
2. Dy. Director (Admn.) of respective Institutes
3. Vice-President (Marketing), M/s HLL Lifecare Ltd. Thiruvanthapuram, Kerala
4. Manager (Defence Pharma Division), M/s HLL Lifecare Ltd. O/o Noida, UP

Copy for information to:-

1. PSO to Secretary (HFW);
2. PPS to JS(PMSSY.
3. O/o DS (RK), PMSSY
4. US (PMSSY-V)

F. No. D.32020/1/2022-DM Cell/Mobile Hospital (part)
Government of India
Ministry of Health & Family Welfare
(Disaster Management Cell)

Nirman Bhawan, New Delhi
Dated the 27th February, 2025

OFFICE MEMORANDUM

Ministry of Health & Family Welfare, as approved under Pradhan Mantri Ayushman Bharat Health Infrastructure Mission (PM-ABHIM), provides for procurement and operationalization of fifty Bharat Health Initative for Sahyog, Hita and Maitri (BHISHM) cubes at identified Central Government hospitals/institutes to provide on-site emergency clinical care to disaster affected communities.

2. In this regard, is to inform that this Ministry has identified twenty- two AIIMSs/INIs under PMSSY/INI for placement of BHISHM Cubes, for which the institutes have shared the details of nodal officers for the same. Further, a demonstration workshop was also organized on 26th & 27th April, 2024 for the representatives of the twenty-two institutes on operational aspects of the BHISHM Cubes.

3. Going ahead, this Ministry has identified M/s HLL Lifecare Ltd. as executing agency for procurement and supply of BHISHM Cubes at twenty-two identified AIIMS/INIs and finalized the number of BHISHM Cubes allocated for each institute along with associated phase-wise distribution for the same.

4. The details of the phase-wise distribution and allocation of BHIHSM Cubes to each institute is enclosed herewith as **Annexure I** for ready reference. Details of roles and responsibilities of institutes is detailed at **Annexure II**. Further, the Standard Operating Procedure for logistics is also enclosed for ready reference of the institutes.

5. Queries, if any, with respect to procurement and deployment of BHISHM Cubes may be communicated to Mr. Vishal Agarwal, Manager (Defence Pharma Division), M/s HLL Lifecare Ltd., (Mob: 7824001064; Email: vishalagarwal@lifecarehll.com).

6. This issues with the approval of competent authority.

DS(AK)/DS(DM-I)

Pradeep Khasnobis

(Dr. Pradeep Khasnobis)
DDG, DM Cell, MoHFW
Tel: 011-23063230

To:

- Nodal Officers of identified Central Government Hospitals/Institutes (as detailed at **Annexure**)

Copy to:

1. Director/Executive Director of identified Central Government Hospitals/Institutes (as detailed at Annexure)
2. Vice-President (Marketing), M/s HLL Lifecare Ltd., Thiruvananthapuram, Kerala
3. Manager (Defence Pharma Division), M/s HLL Lifecare Ltd, O/o Noida, Uttar Pradesh

Copy for information to:

1. Sr. PPS to AS (PH &P)
2. Sr. PPS to AS (RS)
3. Sr. PPS to JS (NE and Hospital), MoHFW
4. Sr. PPS to JS (INI & PMSSY), MoHFW

Annexure

Phase-wise distribution and allocation of BHISHM Cubes to twenty-two identified Central Government institutes/hospitals:

S. No.	Zone	Hospital/Institute	State/UT	Quantity of BHISHM Cubes
Phase I				
1	North Zone	AIIMS, Delhi*	Delhi	3
2		AIIMS, Rishikesh	Uttarakhand	2
3		AIIMS, Bilaspur	Himachal Pradesh	2
4		AIIMS, Gorakhpur	Uttar Pradesh	2
5		AIIMS, Vijaypur	Jammu	2
6	South Zone	AIIMS, Mangalagiri	Andhra Pradesh	3
7	West Zone	AIIMS, Jodhpur	Rajasthan	3
8		AIIMS, Rajkot	Gujarat	2
9	East Zone	AIIMS, Kalyani	West Bengal	2
10	Central Zone	AIIMS, Bhopal	Madhya Pradesh	2
11	North East Zone	North Eastern Indira Gandhi Regional Institute of Health & Medical Sciences (NEIGRIHMS)	Meghalaya	2
Total				**25**
Phase II				
1	North Zone	AIIMS, Raebareli	Uttar Pradesh	2
2		AIIMS, Bathinda	Punjab	2
3		Postgraduate Institute of Medical Education and Research (PGIMER)	Chandigarh	3
4	South Zone	Jawaharlal Institute of Postgraduate Medical Education and Research (JIPMER)	Puducherry	2
5		AIIMS, Bibinagar	Telangana	2
6	West Zone	AIIMS, Nagpur	Maharashtra	2
7	Central Zone	AIIMS, Raipur	Chhattisgarh	3
8	East Zone	AIIMS, Patna	Bihar	2
9		AIIMS, Bhubaneswar	Odisha	3
10		AIIMS, Deoghar	Jharkhand	2
11	North East Zone	AIIMS, Guwahati	Assam	2
Total				**25**

*Nodal Officer from JPNATC, AIIMS, New Delhi to be identified

Annexure II

Roles and responsibilities of institutes receiving BHISHM Cubes

There are diverse range of items contained within the BHISHM Cube, which encompass various categories such as food products, medicines, devices, and equipment. These items can be broadly categorized into 'Expiry and Non-Expiry Items' based on their shelf life.

'Expiry items' may have different shelf lives ranging from 1 year, 2 years, 3 years and more. 'Non-Expiry' category, distinguishes between Non-Battery Operated, Rechargeable, and Battery Operated Items, as well as Hi-End Equipment's. These subcategories require specific maintenance and servicing procedures to ensure optimal functionality and longevity.

Key roles and responsibilities of institutes receiving BHSIHM Cubes are as detailed below:

i. To monitor the expiration dates of items with limited shelf life, proactively use the near expiry items for normal Hospital use and replenish with fresh stock
ii. To ensure that the items requiring Cold Chain to be stored and maintained at the required temperature in a refrigerator, until required.
iii. Use the Battery Operated Items at least once every six months, even if they are not required for immediate use.
iv. For battery-operated items specifically, it is recommended to remove the batteries from the devices when not in use.
v. To ensure availability of all necessary licenses, permits, and consents required by law to store and sell the products, including but not limited to a valid drug license, Narcotic License, PNDT License, AERB License, etc.
vi. To provide the required space for placement of BHISHM Cubes
vii. To ensure Goods Receipt Note to be provided by the authorized Hospital authorities on receipt of the supplied BHISHM CUBE.
viii. To maintain a log book, detailing the complete count of the products and update the same on monthly basis.
ix. To ensure the storage of the laboratory consumables and reagents under the 2 to 8 °C. Also, ensure that medicines are stored in the ambient temperature of 15 to 25 °C, and injectable like Tetanus, are stored in 2 to 8 degree Celsius. A temperature log sheet may be maintained accordingly.

File No. Z-28016/125/2024-PMSSY-V (Computer No. 8283121)
Generated from eOffice by VIKASH KUMAR GUPTA, ASO(VKG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 03/03/2025 10:53 am

DDA AIIMS PATNA <dda@aiimspatna.org>

Instructions on Timely submission of Annual Immovable Property Return under Rule 18 (1) of CCS (Conduct) Rules, 1964 by Executive Directors of AIIMS under PMSSY- regarding.

pmssysection iv <pmssysectioniv@gmail.com> Mon, Mar 3, 2025 at 5:28 PM
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, Executive Director Raebareli <edaiimsrbl@gmail.com>, rajwanshiarvind@hotmail.com, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, shakti810505@gmail.com, AIIMS JAMMU <director@aiimsjammu.edu.in>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, madhabananda@gmail.com, sachimohanty@rediffmail.in
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, "Dr. PRADIP KUMAR" <kpradip10@gmail.com>, dda@aiimskalyani.edu.in, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, Rajeev Sen Roy <rajeevsenroy30@gmail.com>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, dda@aiimsbilaspur.edu.in, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, Administrative Officer <ao.aiimsmadurai@gmail.com>, T Ngamlien <t.ngamlien@icg.gov.in>, Mukesh Kumar <mac.prasad@gmail.com>, ddaaiimsawantipora1@gmail.com, "Dy Director Administration AIIMS, Raebareli" <ddaaiimsrbl@gmail.com>, president@aiimsbhopal.edu.in, Shailesh kumar <shaileshkdr@gmail.com>, swasthyajp1@gmail.com, sub_sinha@hotmail.com, ssinha@aiims.ac.in, dean.sjmc@stjohns.in, snundy@hotmail.com, sravi2008@gmail.com, Chitra Sarkar <sarkar.chitra@gmail.com>, ddverma26@gmail.com, nkarora@inclentrust.org, president@aiimsbilaspur.edu.in, Yk Gupta <yk.ykgupta@gmail.com>, dr prashant lavania <dr.plavania@gmail.com>, bez_bikki@yahoo.co.in, babulbezbaruah2496@gmail.com, Dr Pramod Garg <pgarg10@gmail.com>, pgarg@aiims.edu, ANKITA MISHRA BUNDELA <js-pmssy-mohfw@gov.in>, "Cc:" <dinesh.kumar14@nic.in>, Taranjeet Singh <taranjeet.singh@nic.in>, Suprava Poddar <sup15.81997@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officials of PMSSY-IV Section at - dinesh.kumar14@nic.in; taranjeet.singh@nic.in; sup15.81997@gov.in;

Regards
PMSSY-IV Section\
Ministry of Health and Family Welfare

2 attachments

document - 2025-03-03..pdf
98K

OM No 11013.17.2023-PP. A-III.14.07.2023 on IPR.pdf
2756K

eF.No. 11013/17/2023-PP-A.III
Government of India
Ministry of Personnel, Public Grievances and Pensions
Department of Personnel and Training
(Personnel Policy Division)
*****

North Block, New Delhi
Dated 14 July, 2023

OFFICE MEMORANDUM

Subject: Instructions on Timely submission of Annual Immovable Property Return by the members of Central Civil Service/Posts

---

Department of Personnel and Training has been issuing instructions on filing of Annual Immovable Property Return of the previous year latest by **31st January** of the following year, by the members of Central Civil Services/Posts, as required under under Rule 18 of CCS (Conduct) Rules, 1964. Sub-rule 1(ii) of Rule 18 of the CCS(Conduct) Rules, 1964 stipulates that *"Every Government servant belonging to any service or holding any post included in Group 'A' and Group 'B' shall submit an annual return in such form as may be prescribed by the Government in this regard giving full particulars regarding the immovable property inherited by him or owned or acquired by him or held by him on lease or mortgage either in his own name or in the name of any member of his family or in the name of any other person".*

2. Accordingly, all Group 'A' and Group 'B' Government servants are required to file Annual Immovable Property Return of the previous year latest by 31st January of the following year invariably. The need for obtaining these returns regularly and making careful scrutiny of the same was reiterated from time to time.

3. Attention, in this regard, is invited to DOPT OM No. 11012/11/2007 dated 14.12.2007 and 27.09.2011 as per which, vigilance clearance, for the purpose of (a) empanelment (b) any deputation for which clearance is necessary, (c) appointments to sensitive posts and assignments to training programmes (except mandatory training), shall be denied to an officer, if he fails to submit his annual immovable property return of the previous year by 31st January of the following year.

4. Attention is also invited to DOPT OM No. 11013/3/2011-Estt.(A) dated 23.09.2013 requesting all Cadre Controlling authorities that the IPRs (to be submitted by 31st January each year) may be placed in public domain by 31st March of that year.

5. Ministries/Departments are, therefore, requested to ensure that these returns are submitted by all Group A and B Officers under their control in respect of every calendar year by 31st January of the next year. It may be impressed upon them that failure on the part of a Government servant to comply with the requirement of the aforesaid rule can form good and sufficient reasons for instituting disciplinary proceedings against him.

6. Further, Ministries/Departments may also ensure that these returns are placed in public domain within the prescribed period of time. Internal Audit may also be conducted by the Ministries/Departments to ensure that these instructions are being followed in letter and spirit.

14/7/23

(Umesh Kumar Bhatia)
Director (Pers. Policy)
Tel. No. +91-11-23094471
Email: uk.bhatia@gov.in

To

All Ministries/Departments (as per standard list)

MOST IMMEDIATE

No. 11012/11/2007-Estt. (A)
Government of India
Ministry of Personnel & Public Grievances & Pensions
(Department of Personnel & Training)

New Delhi,
Dated the 14th December, 2007

OFFICE MEMORANDUM

Subject:- Guidelines regarding grant of vigilance clearance to members of the Central Civil Services/Central Civil posts.

The undersigned is directed to say that the matter regarding guidelines for giving vigilance clearance to members of the Central Civil Services/ Central Civil posts has been reviewed by the Department of Personnel & Training and it has been decided that the following guidelines for the grant of vigilance clearance to the Government servants belonging to the Central Civil Services/ Central Civil posts shall be applicable with immediate effect:

1. These orders regarding accordance of vigilance clearance to members of the Central Civil Services/posts shall be applicable with respect to (a) empanelment (b) any deputation for which clearance is necessary, (c) appointments to sensitive posts and assignments to training programmes (except mandatory training). In all these cases, the vigilance status may be placed before and considered by the Competent Authority before a decision is taken.

2. The circumstances under which vigilance clearance shall not be withheld shall be as under:

a) Vigilance clearance shall not be withheld due to the filing of a complaint, unless it is established on the basis of at least a preliminary inquiry or on the basis of any information that the concerned Department may already have in its possession, that there is, prima facie, substance to verifiable allegations regarding (i) corruption (ii) possession of assets disproportionate to known sources of income (iii) moral turpitude (iv) violation of the Central Civil Services (Conduct) Rules, 1964.

b) Vigilance clearance shall not be withheld if a preliminary inquiry mentioned in 2(a) above takes more than three months to be completed.

...2/-

c) Vigilance clearance shall not be withheld unless (i) the officer is under suspension (ii) a chargsheet has been issued against the officer in a disciplinary proceeding and the proceeding is pending (iii) orders for instituting disciplinary proceeding against the officer have been issued by the Disciplinary Authority provided that the chargesheet is served within three months from the date of passing such order (iv) chargesheet has been filed in a Court by the Investigating Agency in a criminal case and the case is pending (v) orders for instituting a criminal case against the officer have been issued by the Disciplinary Authority provided that the chargesheet is served within three months from the date of initiating proceedings (vi) sanction for investigation or prosecution has been granted by the Competent Authority in a case under the PC Act or any other criminal matter (vii) an FIR has been filed or a case registered by the concerned Department against the officer provided that the charge sheet is served within three months from the date of filing/registering the FIR/case and (viii) The officer is involved in a trap/raid case on charges of corruption and investigation is pending.

d) Vigilance clearance shall not be withheld due to an FIR filed on the basis of a private complaint unless a chargesheet has been filed by the investigating agency provided that there are no directions to the contrary by a competent court of law.

e) Vigilance clearance shall not be withheld even after sanction for prosecution if the investigating agency has not been able to complete its investigations and file charges within a period of two years. However, such vigilance clearance will entitle the officer to be considered only to be appointed to non-sensitive posts and premature repatriation to the parent cadre in case he is on deputation and not for any other dispensation listed in para 1 of this O.M..

3. In cases where complaints have been referred to the administrative authority concerned, and no substantive response has been received from such administrative authority concerned within three months from the date on which the reference was made, the Disciplinary Authority may provide a copy of the complaint to the officer concerned to seek his comments. If the comments are found to be prima facie satisfactory by the Competent Authority, vigilance clearance shall be accorded.

4. Vigilance clearance shall be decided on a case-by-case basis by the Competent Authority keeping in view the sensitivity of the purpose, the gravity

...3/-

of the charges and the facts and circumstances, in the following situations:

a) where the investigating agency has found no substance in the allegation but the Court refuses to permit closure of the FIR.; and
b) where the investigating agency/inquiry officer holds the charges as proved but the competent administrative authority differs, or the converse.

5. While considering cases for grant of vigilance clearance for the purpose of empanelment of members of the Central Civil Services/Central Civil posts of a particular batch, the vigilance clearance/status will continue to be ascertained from the respective Cadre Authority. In all such cases, the comments of the Central Vigilance Commission will be obtained. However, if no comments are received within a period of three months, it will be presumed that there is nothing adverse against the officer on the records of the body concerned.

6. Vigilance clearance will be issued in all cases with the approval of the Head of Vigilance Division for officers upto one level below their seniority in service. In the case of officers of the level of Additional Secretary/Secretary, this will be issued with the approval of the Secretary. In case of doubt, orders of the Secretary will be obtained keeping in view the purpose for which the vigilance clearance is required by the indenting authority.

7. Vigilance clearance will not normally be granted for a period of three years after the currency of the punishment, if a minor penalty has been imposed on an officer. In case of imposition of a major penalty, vigilance clearance will not normally be granted for a period of five years, after the currency of punishment. During the period, the performance of the officer should be closely watched.

8. Insofar as the personnel serving in the Indian audit and accounts Department are concerned, these instructions have been issued after consultation with the Comptroller and Auditor General of India.

9 All the Ministries/Departments are requested to bring the above guidelines for the notice of all concerned for information and compliance.

(P. Prabhakaran)
Deputy Secretary to the Government of India

...4/-

Copy forwarded to :

1. Prime Minister's Office (with reference to their I.D. No. 600/68/13/07-ESII, dated 24.10.2007).
2. Cabinet Secretariat.
3. Ministries/Departments of the Government of India.
4. Secretary, Central Vigilance Commission.
5. .Central Bureau of Investigation, New Delhi
6. Union Public Service Commission, New Delhi
7. Comptroller and Auditor General of India, New Delhi

Copy to:

(i) PS to MOS(PP)
(ii) PPS to Secretary(P)
(iii) PPS to AS(S&V)
(iv) PPS to EO & AS
(v) PS to JS(E)
(vi) PS to JS(V) (w.r.t. AVD Division's O.M. No. 104/33/2005-AVD-I dated 31.10.2007.

(P. Prabhakaran)
Deputy Secretary to the Government of India

No. 11012/11/2007-Estt.A
Government of India
Ministry of Personnel, Public Grievances & Pensions
Department of Personnel & Training

New Delhi, Dated 27th September,2011

OFFICE MEMORANDUM

Subject: **Guidelines regarding grant of 'Vigilance Clearance' to members of Central Civil Services / Posts.**

The undersigned is directed to say that it has been decided by the Government that officers who have not submitted the Annual Immovable Property Returns by the prescribed time would be denied vigilance clearance and will not be considered for empanelment for senior level posts in Government of India.

2. Accordingly, in this Department's OM No. 11012/11/2007-Estt.A dated 14.12.2007, laying down guidelines regarding grant of vigilance clearance to members of Central Civil Services / Posts, in para 2 a new sub-para (f) will be inserted as under:

(f) Vigilance clearance shall be denied to an officer if he fails to submit his annual immovable property return of the previous year by 31st January of the following year, as required under Government of India decisions under Rule 18 of the Central Civil Services (Conduct) Rule, 1964.

(U.S. Chattopadhyay)
Under Secretary to the Government of India

All Ministries / Departments

Copy to:

1. Prime Minister's Office (w.r.t. their I.D. No. 600/31/C/33/2011-ES2, dated 15.03.2011)
2. Cabinet Secretariat
3. Secretary, CVC
4. UPSC
5. C&AG
6. NIC (DOP&T Cell) with the request to upload this O.M. on the website of DOP&T.

F.No. 11013/3/2011-Estt.(A)
Ministry of Personnel, P.G. & Pensions
Department of Personnel & Training
Estt.(A)-III Desk

North Block, New Delhi
Dated 23rd September, 2013

OFFICE MEMORANDUM

Subject: Submission of Immovable Property Returns (IPRs) by officers of Group A Central Services for each year and placing the same in public domain.

The undersigned is directed to refer to this Department's O.M of even no. dated 11/04/2011 requesting all Cadre Controlling authorities to place in public domain the IPRs of Group 'A' Officer for the year 2010 by 31.05.2011.

2. In this connection, it is clarified that this was not intended to be a one-time measure but will be a continuous process. All Cadre Controlling authorities are requested that the IPRs (to be submitted by 31st January each year) may be placed in public domain by 31st March of that year. A report in respect of Group 'A' Service controlled by the Ministry/Department and offices belonging to General Central Service Group 'A' under the Ministry /Department may be sent to this Department by 30th April every year.

(Mamta Kundra)
Joint Secretary to the Government of India

To
1. All Ministries/Departments of the Government of India
2. The Comptroller and Auditor General of India
3. NIC (DOP&T) for placing the circular in website.

DDA AIIMS PATNA <dda@aiimspatna.org>

Fwd: Establishment of dedicated engineering wing to provide technical support and expertise in planning design and execution of sports infrastructure projects.

Director . <director@aiimspatna.org> Tue, Mar 4, 2025 at 1:05 PM
To: DDA AIIMS PATNA <dda@aiimspatna.org>

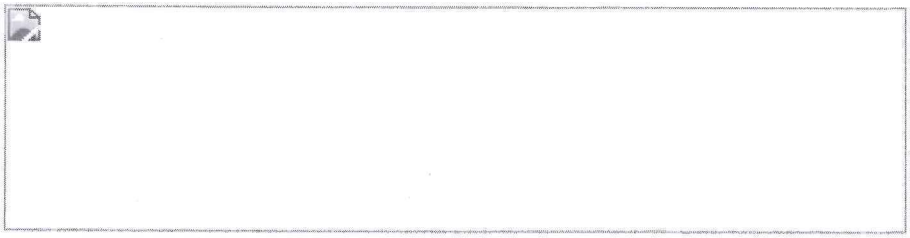
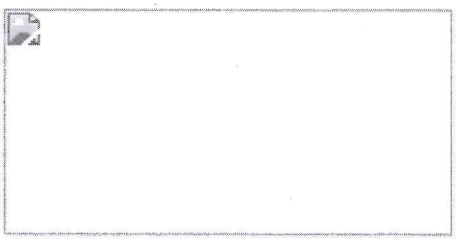
Sd/-
Prof. (Dr.) Saurabh Varshney
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109

---------- Forwarded message ---------
From: **Mr Sourabh** <pmssy5-mohfw@gov.in>
Date: Tue, Mar 4, 2025 at 12:35 PM
Subject: Establishment of dedicated engineering wing to provide technical support and expertise in planning design and execution of sports infrastructure projects.
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Executive Director Raebareli <ed.aiimsrbl@gmail.com>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, Dinesh Singh <director@aiimsbathinda.edu.in>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, ED AIIMS Guwahati <executive-director@aiimsguwahati.ac.in>, ED AIIMS Bilaspur <edaiimsbls@gmail.com>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Director AIIMS Vijaypur <shakti810505@gmail.com>, DDA AIIMS Awantipora <rakeshkumar7123@yahoo.in>, Executive Director AIIMS Rajkot <ed.aiimsrajkot@gmail.com>, Director AIIMS Bibinagar <director.aiimsbbnagar@gmail.com>, Executive Director AIIMS Darbhanga <madhabananda@gmail.com>, Director AIIMS Madurai <drmhraosvims1957@gmail.com>
Cc: Dharm Bir Kumar SIngh <dharmbk.singh@nic.in>, Sourabh <sourabh.12@gov.in>, NARVEER REDHU <narveer.redhu@gov.in>

Respected Sir/Madam,

With reference to the subject cited above, Please find the attachment herewith.

With Regards
PMSSY-V Section
Nirman Bhawan
New Delhi-110011

2 attachments

Letter dated 04-03-25.pdf
85K

Encl__DO Letter 12-02-25.pdf
520K

F.No.-Z-28016/31/2025-PMSSY-V [8322566]
Government of India
Ministry of Health & Family Welfare
Department of Health & Family Welfare
(PMSSY-V Section)
****

Room no. 746-A, Nirman Bhawan, New Delhi
Date 04-03-2025

To

The Director/Executive Directors,

[All AIIMS under PMSSY].

Subject: Establishment of dedicated engineering wing to provide technical support and expertise in planning design and execution of sports infrastructure projects.

Sir/ Madam,

I am directed to enclose a copy of DO letter No.01-11024(08)/5/2024-HO-Infra. dated 12.02.2025 from Ms. Sujata Chaturvedi (Director Genenal, Sports Authority of India), on the subject mentioned above, for appropriate action.

Yours faithfully,

Digitally signed by
Dharm Bir Kumar Singh
Date: 04-03-2025
10:18:45

(Dharm Bir Kumar Singh)
Under Secretary to Govt. of India
Tele: 011-23060006

Encl. : As above

सुजाता चतुर्वेदी, भा.प्र.से.
महानिदेशक
Sujata Chaturvedi, IAS
Director General

सत्यमेव जयते

भारतीय खेल प्राधिकरण
SPORTS AUTHORITY OF INDIA

D.O.No.01-11024(08)/5/2024-HO - Infra **12th February, 2025**

Office of Secretary (Health & FW)
FTS No 4097950
Date 19/02/25

Dear Secretary,

The Sports Authority of India (SAI) has been at the forefront of promoting and developing sports infrastructure across the country to strengthen India's sporting ecosystem. In furtherance of this objective, SAI has now established a dedicated **Engineering Wing** to provide technical support and expertise in the planning, design, and execution of sports infrastructure projects, including Fields of Play (FOPs).

2. The Engineering Wing has been constituted with qualified professionals and experts who will assist State governments, Union Territories, and other stakeholders in ensuring the development of cost-effective and technically sound sports infrastructure. The technical assistance offered by this Wing will include:

- **Preparation of detailed project reports (DPRs)** for new and existing sports infrastructure projects.
- **Development of architectural and structural drawings**, ensuring adherence to national and international standards.
- **Vetting of designs and technical feasibility assessments** to enhance efficiency and sustainability.
- **Preparation of cost estimates**, ensuring optimal utilization of resources.
- **Other related services**

Pl. circulate to all EDs.

Dir (AS)
26/02

3. These services will be extended at a **nominal fee of 0.75% of the estimated project cost**, providing technical assistance accessible to all stakeholders. It is expected that this initiative will facilitate the expeditious and efficient execution of sports infrastructure projects across the country.

4. State governments and other Central/State agencies engaged in the development of sports facilities are encouraged to collaborate with SAI's Engineering Wing to avail of these services. This initiative aims to ensure uniformity and quality in sports infrastructure development, ultimately benefiting athletes and the sporting community of our country.

US (Dharmendra)

5. I request your kind attention to this matter and solicit your support in conveying this initiative to the relevant departments and agencies within your jurisdiction. This will ensure that the expertise of SAI's Engineering Wing for the effective execution of sports infrastructure projects is duly leveraged.

JS (PMSSY)

6. I look forward to your cooperation in this endeavor to strengthen the development of sports infrastructure across the country.

with best wishes,

Yours sincerely,

12/2/25
(Sujata Chaturvedi)

18/2

27/02/2025
SO (PMSSY-V)

To,

Secretaries of all Ministries/Departments of Government of India

ASO (N)
27/2/25

भारतीय खेल प्राधिकरण (युवा कार्यक्रम एवं खेल मंत्रालय), जवाहरलाल नेहरू स्टेडियम परिसर, पूर्वी द्वार नं. 10, लोधी रोड, नई दिल्ली–110003
SPORTS AUTHORITY OF INDIA (Ministry of Youth Affairs & Sports), Jawaharlal Nehru Stadium Complex, East Gate No. 10, Lodhi Road, New Delhi - 110003
Ph.: 91-11-24362720 (O), 24362721 (Fax) E-mail : dg-sai@gov.in

DDA AIIMS PATNA <dda@aiimspatna.org>

Welfare measures undertaken to secure reservation for the purpose of Article 15(4) and Article 16(4) of the Constitution of India for admission in seat in educational institutions and for appointments or posts in the public services under the control of Ministry of Health and Family Welfare, Government of India lor OBCs excluding creamy layer amongst them.

pmssysection iv <pmssysectioniv@gmail.com> Fri, Mar 21, 2025 at 11:12 AM
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, drppjoshi@aiimsnagpur.edu.in, Executive Director Raebareli <edaiimsrbl@gmail.com>, rajwanshiarvind@hotmail.com, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, "Sharma, DN" <sharmadn@aiims.edu>, shakti810505@gmail.com, AIIMS JAMMU <director@aiimsjammu.edu.in>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, madhabananda@gmail.com, sachimohanty@rediffmail.in
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, Rajeev Sen Roy <rajeevsenroy30@gmail.com>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, dda@aiimsrbl.edu.in, "Dy Director Administration AIIMS, Raebareli" <ddaaiimsrbl@gmail.com>, "Dr. PRADIP KUMAR" <kpradip10@gmail.com>, dda@aiimskalyani.edu.in, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, dda@aiimsbilaspur.edu.in, Mukesh Kumar <mac.prasad@gmail.com>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, aps101982@rediffmail.com, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, Administrative Officer <ao.aiimsmadurai@gmail.com>, T Ngamlien <t.ngamlien@icg.gov.in>, ddaaiimsawantipora1@gmail.com, "Cc:" <Dinesh.kumar14@nic.in>, Taranjeet Singh <taranjeet.singh@nic.in>, Suprava Poddar <sup15.81997@gov.in>

Sir/ Madam

Please find the attachment. Circulated as directed.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officials of PMSSY-IV Section at - dinesh.kumar14@nic.in; ; taranjeet.singh@nic.in; sup15.81997@gov.in;

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

Image_737.pdf
938K

F. No. A-14019/08/2023-WPG
Government of India
Ministry of Health and Family Welfare
(W&PG Section)

Nirman Bhawan, New Delhi-110011
Dated 13th March, 2025

OFFICE MEMORANDUM

Subject: Welfare measures undertaken to secure reservation for the purpose of Article 15(4) and Article 16(4) of the Constitution of India for admission in seat in educational institutions and for appointments or posts in the public services under the control of Ministry of Health and Family Welfare, Government of India for OBCs excluding creamy layer amongst them.

A review meeting on the welfare measures undertaken to secure reservation for the purpose of Article 15(4) and Article 16(4) of the Constitution of India for admission in seat in educational institutions and for appointments or posts in the public services under the control of Ministry of Health and Family Welfare (MoHFW), Government of India for OBCs excluding creamy layer amongst them, was held in the National Commission for Backward Classes (NCBC) on 28.02.2025 at 5.00 PM under the Chairpersonship of the Hon'ble Chairperson of NCBC in the Court Room of NCBC at Trikoot-1, Bhikaji Cama Place, New Delhi.

2. During the meeting, the Hon'ble Commission advised MoHFW to ensure maintenance of Reservation Rosters and Reservation Roster Registers in proper manner by the Central Government Hospitals/ Institutes / Organizations.

3. In this regard, attention of all concerned is drawn to the principles laid down by the Department of Personnel and Training (DoPT) for maintenance of Reservation Registers and Reservation Roster Registers. The same is mentioned below with a request to all the Divisions **to ensure compliances with these principles** by all Central Government Hospitals/ Institutes / Organizations under their administrative control:

a. Separate registers/ roster registers shall be maintained for appointments

made by direct recruitment and promotion. In case of promotion, separate registers / roster registers shall be maintained for each mode of promotion viz. limited competitive examination, selection, non-selection, etc.

b. A common register / roster register shall be maintained for permanent appointments and temporary appointments likely to become permanent or to continue indefinitely.

c. A separate register / roster register shall be maintained for purely temporary appointments of 45 days or more, but which have no chance whatever of becoming permanent or continuing indefinitely.

d. Immediately after an appointment is made, the particulars of the person appointed shall be entered in the register / roster register in the appropriate columns and the entry signed by the appointing authority or by an officer authorized to do so.

e. No gap shall be left in completing the register / roster register.

f. The register / roster register shall be maintained in the form of a running account year after year. For example, if recruitment in a year stops at Point 6, recruitment in the following year shall begin from Point 7.

g. If reservation register becomes unwieldy or difficult to manage, a fresh register may be started by applying the method of initial preparation of registers.

h. In case of cadres where reservation is given by rotation, fresh cycle of roster shall be started after completion of all the points in the roster.

i. Since reservation does not apply to deputation/absorption, where the recruitment rules prescribe a percentage of posts to be filled by these methods, such posts shall be excluded for determining reservations.

j. After every recruitment year, an account shall be noted in the reservation register indicating representation of Scheduled Castes/ Scheduled Tribes/ Other Backward Classes and details of backlog reserved vacancies, etc.

4. It is further requested that the Divisions concerned must ensure presence of senior representatives of the Central Government Hospitals/ Institutes / Organizations who are conversant with the subject matter and are in a position to respond adequately to the queries of NCBC in future hearings / meetings. The discrepancies pointed out by the Hon'ble Commission in the Reservation Rosters/ Reservation Roster Registers should also be rectified on priority basis and the information desired by them during the hearings / meetings should be furnished to the Hon'ble Commission expeditiously.

Digitally signed by
Sachin Kumar
Date: 13-03-2025
15:08:46

(Sachin Kumar)
Director (Vigilance) & Liaison Officer for OBCs
Tele No. 011-23061767

To

Joint Secretary (INI)/ Joint Secretary (Hospital)/ Adviser Cost (Drugs Regulation)/ Secretary (NMC)/ Executive Director, NBEMS with reference to the review meeting held at NCBC on 28.02.2025.

Copy to:

i. DGHS
ii. All ASs/ other JSs/ equivalent officers of DoHFW with a request to ensure strict compliance of above principles by all Central Government Hospitals/ Institutes / Organizations under their administrative control.

Copy to (for information):

PSO to Secretary (HFW)

DDA AIIMS PATNA <dda@aiimspatna.org>

Conduct of Emergency Medical Technician Diploma Course as in AIIMS Bilaspur – reg.

Mr Sourabh <pmssy5-mohfw@gov.in> Tue, Apr 15, 2025 at 4:53 PM
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Executive Director Raebareli <ed.aiimsrbl@gmail.com>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, Dinesh Singh <director@aiimsbathinda.edu.in>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, ED AIIMS Guwahati <executive-director@aiimsguwahati.ac.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Director AIIMS Vijaypur <shakti810505@gmail.com>, DDA AIIMS Awantipora <rakeshkumar7123@yahoo.in>, Executive Director AIIMS Rajkot <ed.aiimsrajkot@gmail.com>, Director AIIMS Bibinagar <director.aiimsbbnagar@gmail.com>, Executive Director AIIMS Darbhanga <madhabananda@gmail.com>, Director AIIMS Madurai <drmhraosvims1957@gmail.com>
Cc: DDA BHOPAL <dydir@aiimsbhopal.edu.in>, DDA Bhubaneswar <dda@aiimsbhubaneswar.edu.in>, DDA Jodhpur <dda@aiimsjodhpur.edu.in>, DDA AIIMS Patna <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, DDA AIIMS Rishikesh <dda@aiimsrishikesh.edu.in>, DDA RAEBARELI <ddaaiimsrbl@gmail.com>, DDA NAGPUR <dda@aiimsnagpur.edu.in>, "Dr. DDA AIIMS Kalyani" <kpradip10@gmail.com>, AIIMS DDA Gorakhpur <dda@aiimsgorakhpur.edu.in>, DDA GORAKHPUR <ashwanimahaur@gmail.com>, DDA AIIMS Bathinda <rajeevsenroy30@gmail.com>, DDA AIIMS Deoghar AIIMS Deoghar <dda@aiimsdeoghar.edu.in>, AMRENDRA KUMAR <amrendra.kumar72@gov.in>, DDA AIIMS Madurai <ddamadurai1189@gmail.com>, DDA AIIMS Rajkot <dda.aiimsrajkot@gmail.com>, DDA AIIMS BIBINAGAR <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Guwahati <dda@aiimsguwahati.ac.in>, "DDA AIIMS Vijaypur, Jammu" <ddaaiimsjammu@gmail.com>, ABHIJIT CHAKRABORTY <abhijit.69@gov.in>, tdprao2004 <tdprao2004@gmail.com>, Dharm Bir Kumar SIngh <dharmbk.singh@nic.in>, Mr DEEPAK <deepak.57@gov.in>

Respected Sir/Madam,

With reference to the subject cited above, Please find the attachment herewith.

With Regards
PMSSY-V Section
Nirman Bhawan
New Delhi-110011

2 attachments

Letter dated 15.04.25-.pdf
86K

Curriculum of Emergency Medical Technician Diploma Course of AIIMS Bilaspur.pdf
10077K

No. Z-28016/166/2018-PMSSY-III-Part (2)(8329999)
Government of India
Ministry of Health & Family Welfare
(Department of Health & Family Welfare)
PMSSY V Section

Room No. 746 Á' Wing,
Nirman Bhawan, New Delhi – 110 011.
15-04-2025

To,

The Director / Executive Director
(All AIIMS except Bilaspur)

Subject : Conduct of Emergency Medical Technician Diploma Course as in AIIMS Bilaspur – reg.

Sir/Madam,

Please find enclosed herewith the curriculum of the Emergency Medical Technician Course, being conducted by JIPMER Puducherry which has been started by AIIMS Bilaspur and has been received well for further appropriate action at your end .

Yours faithfully,
Digitally signed by
Dharm Bir Kumar Singh
Date: 15-04-2025
13:04:45

(Dharm Bir Kumar Singh)
Under Secretary to the Government of India
Tel. (O) : 011-230600C

Encl. : AIIMS Bilaspur - Curriculum of Emergency Medical Technician Diploma course.

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Subject: Optimal utilization of medical equipment, infrastructure created through CSR and delivery of specialized services- General guidelines -reg.

2 messages

DDA AIIMS PATNA <dda@aiimspatna.org> Sat, Aug 23, 2025 at 6:03 PM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **pmssysection iv** <pmssysectioniv@gmail.com>
Date: Thu, Apr 18, 2024 at 4:16 PM
Subject: Subject: Optimal utilization of medical equipment, infrastructure created through CSR and delivery of specialized services- General guidelines -reg.
To: <director@aiimsbhopal.edu.in>, <director@aiimsjodhpur.edu.in>, <Director@aiimsraipur.edu.in>, <dir@aiimsrishikesh.edu.in>, <edaiimsrbl@gmail.com>, <director@aiimsmangalagiri.edu.in>, <ed@aiimskalyani.edu.in>, Surekha Kishore <surekhakishore@rediffmail.com>, Singh Dr.Dinesh Kumar <dksbhu@gmail.com>, <director@aiimsdeoghar.edu.in>, <director@aiimsbilaspur.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, <shakti810505@gmail.com>, <director@aiimsguwahati.ac.in>, <ed.aiimsrajkot@gmail.com>, Director JIPMER <director@jipmer.edu.in>
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, <dda@aiimskalyani.edu.in>, Dy Director Administration AIIMS, Raebareli <ddaaiimsrbl@gmail.com>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, <dda@aiimskalyani.ed>, <dda@aiimsgorakhpur.edu.in>, Rajeev Sen Roy <rajeevsenroy30@gmail.com>, <dda@aiimsdeoghar.edu.in>, ddaaiimsbilaspur <ddaaiimsbilaspur@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, <dda@aiimsbhubaneswar.ed>, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, <dda@aiimsnagpur.edu.in>

Sir/ Madam

Please find the attachment.

Note: In case this email requires you to reply, you are requested to reply to all the officers in cc to this email.
Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

document - 2024-04-18T152518.530.pdf
60K

DDA AIIMS PATNA <dda@aiimspatna.org> Wed, Dec 17, 2025 at 1:32 PM

200

To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

[Quoted text hidden]

document - 2024-04-18T152518.530.pdf
60K

Z-28015/27/2024/PMSSY-IV
Government of India
Ministry of Health & Family Welfare
(PMSSY-IV Section)

201-D, Nirman Bhawan, New Delhi.
18-04-2024

To

The Director/Executive Director of all AIIMS under PMSSY MoHFW

Subject: Optimal utilization of medical equipment, infrastructure created through CSR and delivery of specialized services- General guidelines -reg.

Madam/Sir,

I am directed to refer to the subject mentioned above and to say that it has come to the notice of the Ministry that a number of high-end medical equipment are not being utilized optimally due to lack of technicians and Paramedical staff, inconveneince is often faced by patients who come to the Out Patient Department (OPD) due to certain constraints . Further the infrastructure created under CSR is not always optimally utilised and faculty of the institute is often engaged in sundry administrative works which is not their core mandate .

Accordingly in larger public interest , to ensure timely delivery of quality patient care services all Executive Directors are advised to take following action on priroity -

A. Engagement of Paramedical Staff/Technicians/other essential manpower on Out source basis to operationalise all sanctioned Beds and for ensuring timely and quality health care delivery to the people

(i) Proposal for post creation (faculty and non faculty) particulalry of the technicians/ para medical staff where such posts exist in the Standard Staffing Pattern to be sent to the Ministry for seeking approval of the Department of Expenditure .

(ii) Where such posts have been sanctioned and are vacant, these should be filled up by the Institute in mission mode in next 3 months.

(iii) Until the above posts are created or filled up on regular basis and otherwise over and above the posts provided in the Standard Staffing Pattern, if the Institutes require Technicians and Paramedical staff to operationalise all sanctioned beds ,MOT /Labs etc and to provide any specialised services, a

proposal to this effect should be placed before the Standing Finance Committee of the Institute for consideration and approval.

In case of urgency a proposal to this effect may be submitted to the Ministry for consideration and approval of Secreatry HFW / Chairman SFC. Thereafter expost facto approval of SFC can be obatined as and when it is convened .

(iv) All efforts should be made to increase the intake and number of paramedical courses being run by the Institute to meet the growing demand of paramedical staff across various health care institutes.

B. Effective and Optimum Utilization of Infrastructure created from Funds under Corporate Social Responsibility (CSR)

(i) As regards, infrastructure created in the Institute through CSR funding whether it is clinical infrastructure in the nature of Trauma Centre , Burns Centre etc or public convenience like Vishram Sadan etc. or assets like battery operated vehicles, to ensure their effective operationalisation the EDs are advised to submit proposals for

(a) creation of faculty/ non-faculty posts as required

(b) outsourcing services for operationalizing these assets/facilities

so that these can be put to immediate and effective use for the public for which they are meant.

(ii) Procurement of furniture/accessories as is necessary for operationalizing these assets should be made by the Institutes well in time .

Where such procurement is beyond the delegated financial power of the ED, it should be brought as an Agenda to the SFC for consideration and approval .

C. Provision of Public facilitites for OPD Patients

(i) In fully functional 6 AIIMS where the patient load is high and space for OPD is relatively less, immediate measures to be taken to create additional sheds/ waiting areas for patients and their attendants along with provision of adequate toilets, drinking water facility , air coolers etc

(ii) Simultaeously to streamline patient inflow, proposal for setting up of

screening OPD should be exmained and accordingly an Agenda to this effect be placed in the SFC for consideration and approval .

D. <u>Non Assignment of Administrative work to faculty</u>

Doctors/Medical faculty of the institute (both specialists and super specialists) should not be assigned administrative jobs pertaining to procurement, security , horticulture etc as it interferes in the delivery of their core duties of teaching, learning, research and patient care .

To meet the work requirement (i) Vacant posts in the Administration section should be filled up on priority (ii) Hospital Managers may be hired through Outsourcing basis to support DD Admin in the above functions . Proposals may accordingly be placed before the SFC for consideration and approval.

3. This is issued with the approval of Secretary(HFW).

Yours faithfully,

(Dinesh Kumar)
Joint Director
Tele:011-2306 1730

Copy to : DD(A)s of AIIMSs/INIs under MoHFW

Signed by Dinesh Kumar
Date: 18-04-2024 10:59:58

DDA AIIMS PATNA <dda@aiimspatna.org>

Mandatory Security Audit & Certification of Website/Software Applications – Reg.

mn mishra <mnmishra.mohfw@gmail.com> Fri, Apr 25, 2025 at 2:23 PM
To: DDA AIIMS Bhopal <dydir@aiimsbhopal.edu.in>, DDA AIIMS Jodhpur <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Rishikesh <dda@aiimsrishikesh.edu.in>, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, Deputy Director Administration <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, ddaaiimsbilaspur <ddaaiimsbilaspur@gmail.com>, dda@aiimsdeoghar.edu.in, "Recruitment Cell AIIMS, Bathinda" <recruitmentaiimsbathinda@gmail.com>, ddamadurai1189@gmail.com, dda@aiimsnagpur.edu.in, "Dy Director Administration AIIMS, Raebareli" <ddaaiimsrbl@gmail.com>, dda@aiimskalyani.edu.in, dda@aiimsgorakhpur.edu.in, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, ddaaiimsjammu@gmail.com, t.ngamlien@icg.gov.in, ddaaiimsawantipora1@gmail.com
Cc: ShriRajKumar Under Secretary <raj.kumar28@nic.in>, arvind.thakur@nic.in, ANKITA MISHRA BUNDELA <js-pmssy-mohfw@gov.in>

Dear Sir/Madam,

This is to bring to your kind attention that, in line with cybersecurity guidelines issued by CERT-In and the Ministry of Health & Family Welfare (MoHFW), it is ***mandatory for all AIIMS institutions*** *to ensure that their* ***websites and software applications undergo a comprehensive security audit*** *through CERT-In empaneled agencies.*

To maintain a secure digital ecosystem and protect sensitive health and administrative data, all AIIMS institutes are requested to:

1. ***Conduct a Security Audit*** *of all public-facing and internal software applications, websites, and portals.*
2. *Ensure the audit is performed by a* ***CERT-In empaneled security agency.***
3. ***Obtain a Security Audit Compliance Certificate*** *upon successful testing.*
4. *Submit the security audit certificate to the e-Health, Ministry of Health and Family Welfare by 30th April 2025.*

Kindly treat this as urgent and high priority. In case the audit has already been conducted recently (within the last 6 months), a copy of the latest certificate may be shared.

For any clarifications or support regarding the empaneled agencies or audit process, please feel free to contact the Cyber Security Cell.

We seek your cooperation in making our healthcare digital infrastructure safe and compliant.

Regards,
Er.M.N.Mishra,
IT Consultant,PMSSY,
Ministry of Health and Family Welfare,
Mob:7982125857

Z-28016/29/2025-PMSSY-I []
Government of India
Ministry of Health & Family Welfare
PMSSY-I

Nirman Bhawan, New Delhi
Dated: 28-04-2025

To

Directors/Executive Directors
All AIIMS

Subject: Undertaking Analysis of Patient Feedback and Implementation of Corrective Measures across all AIIMS-reg.

Sir/Ma'am

I am directed to refer to the directions of the Hon'ble Health and Family Welfare Minister (HFM)on the subject mentioned above and to state that provision of patient centric health care services is a mandate of all AIIMS beings Institutes of national Importance , accordingly all Executive Directors of AIIMS are advised to undertake a bi monthly comprehensive analysis of patient feedback received in the Institute regarding the services being provided by the Institute to identify areas requiring improvement and to initiate necessary corrective actions to address the concerns under intimation to the Ministry .

Yours faithfully,

Digitally signed by Raj Kumar
Date: 28-04-2025 09:31:22

(Raj Kumar)
Deputy Secretary to GoI
Tele: 011-23063178

Copy to:

(i) Deputy Directors (Admin), all AIIMS

Copy for Information to:

(i) PS to Hon'ble HFM
(ii) PPS to JS (PMSSY)

DDA AIIMS PATNA <dda@aiimspatna.org>

Procurement of Medicines and Medical Devices from Hindustan Antibiotic Ltd., Pune-reg

GUNJAN SHARMA <gunjan.s@gov.in> Wed, Apr 30, 2025 at 4:07 PM
To: director <director@aiimsbhopal.edu.in>, director <director@aiimsbhubaneswar.edu.in>, director <director@aiimsjodhpur.edu.in>, director <director@aiimspatna.org>, director <director@aiimsraipur.edu.in>, director <director@aiimsrishikesh.edu.in>, director <director@aiimsmangalagiri.edu.in>, directoraiimsnagpur <directoraiimsnagpur@gmail.com>, drppjoshi <drppjoshi@aiimsnagpur.edu.in>, edaiimsrbl <edaiimsrbl@gmail.com>, rajwanshiarvind <rajwanshiarvind@hotmail.com>, ed <ed@aiimskalyani.edu.in>, executivedirector <executivedirector@aiimsgorakhpur.edu.in>, director <director@aiimsdeoghar.edu.in>, Director Bibinagar <director@aiimsbibinagar.edu.in>, director <director@aiimsbilaspur.edu.in>, sharmadn <sharmadn@aiims.edu>, shakti810505 <shakti810505@gmail.com>, director <director@aiimsjammu.edu.in>, drmhraosvims1957 <drmhraosvims1957@gmail.com>, director <director@aiimsguwahati.ac.in>, madhabananda <madhabananda@gmail.com>, sachimohanty <sachimohanty@rediffmail.in>
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, dda <dda@aiimsjodhpur.edu.in>, dda <dda@aiimspatna.org>, dda <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, dda <dda@aiimsrbl.edu.in>, kpradip10 <kpradip10@gmail.com>, dda <dda@aiimskalyani.edu.in>, dda <dda@aiimsgorakhpur.edu.in>, rajeevsenroy30 <rajeevsenroy30@gmail.com>, dda <dda@aiimsbathinda.edu.in>, dda <dda@aiimsdeoghar.edu.in>, officeaiimsdeoghar <office.aiimsdeoghar@gmail.com>, ddaaiimsbibinagar <dda.aiimsbibinagar@gmail.com>, dda <dda@aiimsbibinagar.edu.in>, dda <dda@aiimsbilaspur.edu.in>, macprasad <mac.prasad@gmail.com>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, aoaiimsmadurai <ao.aiimsmadurai@gmail.com>, tngamlien <t.ngamlien@icg.gov.in>, ddaaiimsawantipora1 <ddaaiimsawantipora1@gmail.com>, ddapgi <ddapgi@gmail.com>, krishanagoyal <krishana.goyal@jipmer.edu.in>, DDA <DDA@aiims.edu>, Shri Raj Kumar Deputy Secretary <raj.kumar28@nic.in>, Ravi Kumar <ravi.kumar89@gov.in>

Sir/Ma'am

Please find attachment on the subject cited above for necessary action.

Thanks & Regards
Gunjan Sharma, Central Secretariat Service (CSS)
Assistant Section Officer
PMSSY-I
Ministry of Health & Family Welfare
Govt. of India

Please consider your environmental responsibility. Before printing this e-mail message, ask yourself whether you really need a hard copy.

2 attachments

letter to all AIIMS.pdf
81K

enclosure.pdf
2943K

Z-28016/32/2025-PMSSY-I (E0-8332606)
Government of India
Ministry of Health & Family Welfare
(PMSSY-I Section)

Nirman Bhawan, New Delhi-110001
Date:30-04-2025

To,

Executive Director
All New AIIMS under PMSSY.

Subject: Procurement of Medicines and Medical Devices from Hindustan Antibiotic Ltd., Pune-reg.

I am directed to forward a copy of OM. No. Z.28015/29/2023-Proc.I (EPW) dated 09.04.2025 enclosing therewith a copy of the letter received from Hindustan Antibiotics Ltd. (HAL) Pune No. HAL/24-25 dated 14.1.2025 alongwith a copy of the Pharmaceutical Purchase Policy (PPP-2013) and an Office Memorandum dated 10.12.2013, regarding the procurement of medicines and medical devices from HAL.

2. The above documents are being shared for your information and for taking necessary action in compliance with the extant rules and guidelines laid down under the said policy.

Encl: As above

Yours faithfully,

Digitally signed by Raj Kumar
Date: 30-04-2025 10:15:39

Deputy Secretary to the Government of India
Tel: 011-23063178

F.No.Z.28015/29/2023-Proc.I(EPW) 8230935
Government of India
Ministry of Health & Family Welfare
Department of Health and Family Welfare
[Procurement-I (EPW) Section]

Nirman Bhawan, New Delhi
Dated: April, 2025

OFFICE MEMORANDUM

Subject: Procurement of Medicines and Medical Devices from Hindustan Antibiotic Ltd., Pune -reg.

The undersigned is directed to forward herewith a copy of letter from Hindustan Antibiotics Ltd. (HAL), Pune No. HAL/24-25 dated 14.01.2025 alongwith a copy of the Pharmaceutical Purchase Policy (PPP-2013) and an OM dated 10.12.2013 regarding Procurement of Medicines and Medical Devices from Hindustan Antibiotics Limited for information and necessary action in compliance with extant rules.

(Encl: As above)

Digitally signed by
LAVKESH SEHGAL
Date: 09-04-2025
14:44:36

(Lavkesh Sehgal)
Under Secretary to Government of India
Phone: 011-23061875

To,

All procuring entities as per list.

नीरजा सराफ
प्रबन्ध निदेशक

NIRJA SARAF
Managing Director

हिन्दुस्तान एंटिबायोटिक्स लि.
(भारत सरकार का उद्यम)
पिंपरी, पुणे - 411 018.
महाराष्ट्र, भारत

HINDUSTAN ANTIBIOTICS LTD.
(A GOVT. OF INDIA ENTERPRISE)
PIMPRI, PUNE - 411 018.
MAHARASHTRA, INDIA

REF: HAL /24-25/

Date: 14.01.2025

To,

Shree J. P. Nadda ji
Hon'ble Minister of Health
& Family Welfare
Govt. of India
Nirman Bhawan
NEW DELHI – 110011.

Sub: Regarding Procurement of Medicines and Medical Devices from Hindustan Antibiotics Ltd., Pune.

Respected Sir,

Hindustan Antibiotics Limited (HAL), a Govt. of India Enterprise, situated in the state of Maharashtra at Pimpri, Pune. We are the first Central Public Sector Enterprise (CSPE) in Pharma sector in the country and functioning under the Department of Pharmaceuticals, Ministry of Chemicals and Fertilizers, Govt. of India. We are one of the major suppliers of quality life saving medicines to various Central and State Govt. Institutions.

Govt. of India has sanctioned the Pharmaceutical Purchase Policy (PPP 2013) for procurement of 103 essential listed medicines by all the procurement authorities of Govt., Semi Govt., Autonomous Bodies mandatorily from Pharmaceutical CPSE companies. The policy has been further renewed by the Union cabinet with the same terms & adding another product i.e. **HALRUB** (Alcoholic Hand Disinfectant) vide Office Memorandum dt. 04/12/2019 **(Annexure-I)**. Thus, the total no. 0f 104 items are reserved for Pharma CPSE Companies only. The said policy would be applicable to purchases by Central Government Departments, their Public Sector Undertakings and Autonomous Bodies etc & State Governments under Health programmes funded by Government of India such as NHM, NRHM etc.

Secretary (Health)

HAL with its integrated smart digital platform has launched a network of '**Health ATMs**' known as HAL Cloud Clinic (HCC). It offers instant health check-up **of various important health parameters like Hypertension, Anemia, Diabetes, Oxygen Saturation (SpO2), BMR, BMI, Lipid Profile, HbA1c, ECG etc. along with various rapid Tests such as Malaria, Dengue, Typhoid, Routine Urine, Blood Grouping, Covid Antigen.** These Health ATMs are integrated with various government technological advancements like ABHA Health Id & E-Sanjeevani for telemedicine. It maintains Digital Health profile of each patient and also provides Data Analytics dashboard for disease surveillance & patient demographics. Our HCC machine has the ability to track health over time from the cloud. After checkup, health details are instantly sent to the patient through his registered E Mail & WhatsApp.

Features:
Instant test results
Digital health record of patients
Secure and Reliable
Instant Health Report
Data Analytics Dashboard
Low running costs
Works without internet and electricity
Easy to install and operate with minimum training

फोन (कार्यालय) : (020) 27421929 I फॅक्स : (020) 27425327 I वेबसाईट : www.hindantibiotics.in I ई-मेल : md.hapune@rediffmail.com
TELEPHONE (OFF.) : (020) 27421929 I FAX : (020) 27425327 I Website : www.hindantibiotics.in I E-mail : md.hapune@rediffmail.com
CIN - U24231MH1954 PLC 009265
CIN: "U24231MH1954GOI009265" email id:md@halpune.in

List of Parameters Covered:

Sugar	Body Water
Skeleton Muscle	Hemoglobin
Muscle Mass	Blood Grouping
Bone Mass	Covid Antigen
Protein	Vision Test
BMR (Basil Metabolic Rate)	Body Temperature
Metabolic Age	NI BP (Blood Pressure)
Fat Free Weight	Spo2
Health Score	Pulse
Total Cholesterol (TC)	Height
High density Lipoprotein Cholesterol (HDL)	Body Weight
Triglycerides (TG)	BMI (Body mass index)
Low density Lipoprotein Cholesterol (LDL)	Body Fat
TC/HDL Ratio	Physique
HBA1c	Subcutaneous Fat
Rapid tests	Visceral Fat

Our Health Kiosk is installed & functioning successfully in various States such as Uttar Pradesh, Maharashtra, etc., & at various prestigious Institutions. **The Health ATM Machine can be installed at various Health Centers, Govt. Hospitals, Public places all over India.**

We would therefore, urge for your kind initiative in the matter for procurement of medicines as well as Health ATM, which would help common citizens to get quality medicines and know their health status by tracking down signs of various health ailments which can make a significant impact on preventive healthcare.

Thanking you.

Yours Sincerely,

(NIRJA SARAF)
MANAGING DIRECTOR

1576-HO
13/12/13

No.50(9)/2010-PI-IV
Government of India
Ministry of Chemicals & Fertilizers
Department of Pharmaceuticals

Shastri Bhawan, New Delhi
10th December, 2013

OFFICE MEMORANDUM

Sub: Pharmaceuticals Purchase Policy (PPP) for products of Pharma Central Public Sector Enterprises (CPSEs) and their subsidiaries.

The undersigned is directed to say that the Union Cabinet in its meting held on 30.10.13 has approved the Pharmaceuticals Purchase Policy in respect of 103 medicines manufactured by Pharma CPSEs and their subsidiaries. The list of 103 medicines is enclosed. The salient features of PPP are as under:-

i. Pharmaceuticals Purchase Policy in respect of 103 medicines would be valid for a period of five years from the date of issue of orders by Department of Pharmaceuticals.

ii. Pharmaceuticals Purchase Policy will extend only to Pharma CPSEs under the administrative control of Department of Pharmaceuticals such as Indian Drugs and Pharmaceuticals Limited (IDPL), Hindustan Antibiotics Limited (HAL), Bengal Chemicals and Pharmaceuticals Limited (BCPL), Karnataka Antibiotics and Pharmaceuticals Limited (KAPL) and Rajasthan Drugs and Pharmaceuticals Limited (RDPL) and their subsidiaries where Government of India owns 51% or above shares.

iii. This would be applicable to purchases by Central Government departments, their Public Sector Undertakings, and Autonomous Bodies, etc. This would also be applicable to purchase of medicines by State Governments under Health Programmes funded by Government of India such as National Rural Health Mission etc.

iv. The pricing of the products would be done by National Pharmaceutical Pricing Authority (NPPA) using the cost based formula, as mentioned in the Drugs Price Control Order, 95. Uniform discount of 16% would be extended to all products. All the taxes, whatsoever, would have to be passed on to buyers.

v. Annual revision of prices would be linked to Wholesale Price Index as per provisions contained in Drugs Prices Control Order, 2013.

vi. The procuring entity would purchase from Pharma CPSEs and their subsidiaries subject to their meeting Good Manufacturing Practices (GMP) norms as per Schedule 'M' of the Drugs & Cosmetic Rules.

-1-

vii. In case Pharma CPSEs and their subsidiaries fail to supply the medicines, the procuring entity would be at liberty to make purchases from other manufacturers. If the Pharma CPSEs or their subsidiaries fail to perform as per the purchase order, they would also be subject to payment of liquidated damages or any other penalty as per the terms of the contract.

viii. The list of medicines may be reviewed and revised by the Department of Pharmaceuticals as per requirement.

2. All Ministries/Departments are requested to immediately bring the contents of this O.M. to the notice of all concerned officers in the Ministries/Departments, States, CPSEs, Autonomous bodies and other organizations under their administrative control for following the PPP in respect of products of Pharma CPSEs and their subsidiaries.

(Monika Verma)
Director
Tel: 23389866

1. All Secretaries of the Ministries/Departments in the Government of India
2. All Principal Secretaries/Secretaries, Health, State Governments.
3. All Financial Advisers of the Ministries/Departments, Government of India
4. Chairman, National Pharmaceuticals Pricing Authority
5. Managing Directors of Pharma CPSEs (IDPL, HAL, BCPL, KAPL, RDPL).
6. Chief Executives of Public Sector Undertakings / Autonomous Organizations / Bodies etc.

Copy to:

1. The Prime Minister's Office, South Block, New Delhi.
2. Cabinet Secretariat, New Delhi. This has reference to their O.M. No. 41/CM/2013(i) dated 5.11. 2013.
3. Department of Public Enterprises (Shri O.P. Rawat, Secretary) It is requested that contents of this O.M. may specifically be brought to the notice of the Chief Executives of PSUs, Autonomous Bodies, etc.
4. PS to MoS (IC)(C&F)
5. PPS to Secretary (Pharmaceuticals)

(Monika Verma)
Director
Tel: 23389866

LIST OF 103 MEDICINES

	CAPSULES
1	AMOXYCILLIN IP
2	AMOXYCILLIN IP+ CLOXACILLIN IP
3	AMPICILIN IP
4	B-COMPLEX+VIT.-C & ZINC
5	CEPHALEXIN IP
6	DOXYCYCLINE IP
7	FLUCONAZOLE
8	OMEPRAZOLE IP
9	OMEPRAZOLE+DOMPERIDONE
10	CEFADROXIL
11	TETRACYCLINE
	TABLETS
12	ACECLOFENAC + PARACETAMOL
13	ACECLOFENAC 100MG
14	ALBENDAZOLE
15	AMLODEPIN
16	AMOXYCILLIN+CLAVULANIC ACID
17	ASCORBIC ACID IP
18	ATENOLOL
19	ATORVASTATIN
20	AZITHROMYCIN
21	CALCIUM + VITAMIN D3
22	CEFIXIME TABS./ CAPS
23	CEFPODOXIME PROXETIL
24	CEFUROXIME AXETIL
25	CETRIZINE HCL BP
26	CETRIZINE+PARACETAMOL+PHENYL EPHERIN
27	CHLOROQUINE PHOSPHATE IP
28	CIPROFLOXACIN + TINIDAZOLE
29	CIPROLOXACIN IP
30	CO-TRIMOXAZOLE IP
31	DICLOFENAC SODIUM
32	DICYCLOMINE + PARACETAMOL
33	DOMPERIDONE
34	ERYTHROMYCIN STERATE IP
35	IBUPROFEN IP
36	LEVOCETRIZINE
37	LEVOFLOXACIN

-3-

38	LOSARTAN
39	METRONIDAZOLE IP
40	NIMESULIDE
41	NORFLOXACIN + TINIDAZOLE
42	NORFLOXACIN IP
43	OFLOXACIN
44	OFLOXACIN + ORNIDAZOLE
45	ORAL CONTRACEPTIVE PILLS
46	PANTOPRAZOLE
47	PARACETAMOL
48	PARACETAMOL IP + DICLOFENAC SODIUM
49	PARACETAMOL+ IBUPROFEN
50	PENICILLIN V
51	POLYVITAMIN PROPHYLACTIC(NFI)
52	RANITIDINE HCL IP
53	ROXITHROMYCIN
54	METFORMIN
55	SPARFLOXACIN
56	TINIDAZOLE
57	VITAMIN B.COMPLEX (PROPHYLACTIC(NFI)
	SUSPENSION / SYRUP
58	ALBENDAZOLE SUSP.
59	AMOXYCILLIN DRY SYP.
60	CETRIZINE SYRUP
61	COTRIMOXAZOLE SUSP.
62	COUGH SYP. EACH 5 ML CONTAINS- CPM IP : 3MG +AMMONIUM CHLORIDE IP:110MG+SODIUM CITRATE IP :46MG+MENTHOL IP:.9MG
63	COUGH SYP. EACH 5 ML CONTAINS- DYPHENHYDRAMINE HCL:14MG +AMMONIUM CHLORIDE IP:135MG+SODIUM CITRATE IP :57MG+MENTHOL IP:.9MG
64	DOMPERIDONE SUSP.
65	PARACETAMOL SYP.
66	VITAMIN A SOLUTION IP
	ORAL POWDER
67	ORAL REHYDRATION SALT (WHO FORMULA)
	EXTERNAL LOTION / SOLUTION
68	GLUTARALDEHYDE

-4-

69	CHLORHEXIDINE GLUCONATE SOLUTION
	OINTMENT
70	CLOTRIMAZOLE OINTMENT
71	DICLOFENAC GEL.
72	POVIDONE IODINE SOLUTION / OINTMENT)
73	SILVER SULPHADIAZINE
	I.V.FLUID(INFUSION)
74	CIPROFLOXACIN
75	LEVOFLOXACIN IV
76	MANNITOL
77	METRONIDAZOLE
78	PLAZMA VOLUME EXPENDER
79	RINGER LACTATE I.V.
	DRY POWDER / LIQUID INJECTABLES
80	AMIKACIN
81	AMOXICILLIN SODIUM + CLAVULANATE POTASSIUM
82	AMPICILLIN IP
83	AVS LIQUID (LYFOLYSED)
84	BENZATHENE PENICILLIN
85	BENZYLE PENICILLIN IP
86	CEFEPIME
87	CEFOPERAZONE
88	CEFOPERAZONE + SULBACTAM
89	CEFOTAXIME SODIUM USP
90	CEFOTAXIME SODIUM+SULBACTAM
91	CEFTAZADIME
92	CEFTRIAXONE
93	CEFTRIAXONE+SULBACTAM
94	DICLOFENAC SODIUM
95	ETO-THEOPHYLLINE
96	ATROPIN INJ.
97	FRUSEMIDE
98	GENTAMYCIN IP
99	MEROPENEM INJ.
100	PENTAZOCIN
101	PIPERACILLIN+TAZOBACTAM
102	RANITIDINE IP
	TABLETS
103	GLIMEPIRIDE (1mg/2mg)

-5-

DDA AIIMS PATNA <dda@aiimspatna.org>

Temporary downgrading of post of Financial Advisor (FA) (Pay Level 13) to Senior Accounts Officer (Pay Level 11) – reg

3 messages

pmssysection iv <pmssysectioniv@gmail.com> Wed, May 7, 2025 at 11:37 AM
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, drppjoshi@aiimsnagpur.edu.in, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, "Prof. Dr. D.K. Singh, Director" <director@aiimsbathinda.in>, Executive Director AIIMS Rajkot <ed.aiimsrajkot@gmail.com>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, sachimohanty@rediffmail.in, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, "Sharma, DN" <sharmadn@aiims.edu>
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, "Dr. Pradip Kumar" <kpradip10@gmail.com>, dda@aiimskalyani.edu.in, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, Rajeev Sen Roy <rajeevsenroy30@gmail.com>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, dda@aiimsbilaspur.edu.in, Mukesh Kumar <mac.prasad@gmail.com>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, aps101982@rediffmail.com, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, Administrative Officer <ao.aiimsmadurai@gmail.com>, ddaaiimsawantipora1@gmail.com, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, ":" <Ak.biswas57@nic.in>, Vaishali Vinayak <vaishali.vinayak@gov.in>, Amit Batra <amit.batra@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officers of PMSSY-IV Section at - arvind.thakur@nic.in; ak.biswas57@nic.in; vaishali.vinayak@gov.in; amit.batra@gov.in

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

3 attachments

- **Letter (277).pdf** 94K
- **Encl 1 (11).pdf** 4249K
- **Encl 2 (14).pdf** 491K

Director . <director@aiimspatna.org> Tue, May 13, 2025 at 11:18 AM
To: DDA AIIMS PATNA <dda@aiimspatna.org>

Sd/-
Prof. (Dr.) Saurabh Varshney
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109

[Quoted text hidden]

3 attachments

Letter (277).pdf
94K

Encl 1 (11).pdf
4249K

Encl 2 (14).pdf
491K

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, May 15, 2025 at 9:40 AM
To: Amit Kumar Sinha <amit.sinha@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507
[Quoted text hidden]

3 attachments

Letter (277).pdf
94K

Encl 1 (11).pdf
4249K

Encl 2 (14).pdf
491K

Z-28015/57/2023-PMSSY-IV(8243506)
Government of India
Ministry of Health & Family Welfare
(PMSSY-IV Section)

Room No. 745-A, Nirman Bhawan, New Delhi
Dated the 06-05-2025

To,

Executive Director (ED) of new AIIMS (Bhopal, Bhubaneswar, Patna, Nagpur, Kalyani, Gorakhpur, Bathinda, Bilaspur, Deoghar, Rajkot, Madurai, Awantipora and Raipur)

Subject: Temporary downgrading of post of Financial Advisor (FA) (Pay Level 13) to Senior Accounts Officer (Pay Level 11) – reg

Sir/Madam,

I am directed to refer to this Ministry's letter of even no dated 12.03.2024 on the subject cited above and to say that since Sr. Accounts Officer is a Non Faculty Group A Post, the criteria of point 5 of letter of even no dated 12.03.2024 regarding nomination of a member from the Ministry of Health and Family Welfare in the interview panel, gets covered under the composition of the Selection Committee at Para-7 of the guidelines of Circular No. Z-28016/24/2014-SSH dated 01.05.2015 (copy enclosed).

2. Concerned new AIIMS are hereby advised to recruit Sr Accounts Officer as mentioned in letter of even no dated 12.03.2024 by making use of the guidelines of Circular No Z-28016/24/2014-SSH dated 01.05.2015.

Encl(2):

i. letter of even no dated 12.03.2024
ii. Circular No Z-28016/24/2014-SSH dated 01.05.2015

Yours faithfully

Digitally signed by
ARUN KUMAR BISWAS
Date: 06-05-2025
19:02:47

(Arun Kumar Biswas)
Under Secretary to the Government of India
Tel:011-23061343
ak.biswas57@nic.in

Copy to: Deputy Director(Admin) of new AIIMS (Bhopal, Bhubaneswar, Patna, Nagpur, Kalyani, Gorakhpur, Bathinda, Bilaspur, Deoghar, Rajkot, Madurai, Awantipora and Raipur)

DDA AIIMS PATNA <dda@aiimspatna.org>

Fwd: Delivery Status Notification (Failure)

2 messages

pmssysection iv <pmssysectioniv@gmail.com> Mon, May 19, 2025 at 1:03 PM
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, drppjoshi@aiimsnagpur.edu.in, Executive Director Raebareli <edaiimsrbl@gmail.com>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, "Sharma, DN" <sharmadn@aiims.edu>, "Dr.Shakti kumar Gupta" <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, madhabananda@gmail.com, sachimohanty@rediffmail.in
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, Rajeev Sen Roy <rajeevsenroy30@gmail.com>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, dda@aiimsrbl.edu.in, "Dy Director Administration AIIMS, Raebareli" <ddaaiimsrbl@gmail.com>, "Dr. Pradip Kumar" <kpradip10@gmail.com>, dda@aiimskalyani.edu.in, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, dda@aiimsbilaspur.edu.in, Mukesh Kumar <mac.prasad@gmail.com>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, aps101982@rediffmail.com, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, Administrative Officer <ao.aiimsmadurai@gmail.com>, T Ngamlien <t.ngamlien@icg.gov.in>, ddaaiimsawantipora1@gmail.com, ":" <Ak.biswas57@nic.in>, Vaishali Vinayak <vaishali.vinayak@gov.in>, Amit Batra <amit.batra@gov.in>

Sir/ Madam

Kindly ignore the previous mail. Please find the attachment.
Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officers of PMSSY-IV Section at - arvind.thakur@nic.in; ak.biswas57@nic.in; vaishali.vinayak@gov.in; amit.batra@gov.in
Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

---------- Forwarded message ---------
From: **Mail Delivery Subsystem** <mailer-daemon@googlemail.com>
Date: Mon, May 19, 2025 at 12:22 PM
Subject: Delivery Status Notification (Failure)
To: <pmssysectioniv@gmail.com>

Address not found

Your message wasn't delivered to **dda@aiimsrbl.edu.in** because the address couldn't be found, or is unable to receive

mail.

The response from the remote server was:

```
550 #5.1.0 Address rejected.
```

3 attachments

Letter (292).pdf
91K

Encl (60).pdf
3181K

Encl (61).pdf
1080K

DDA AIIMS PATNA <dda@aiimspatna.org> Tue, May 20, 2025 at 3:46 PM
To: Amit Kumar Sinha <amit.sinha@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507
[Quoted text hidden]

3 attachments

Letter (292).pdf
91K

Encl (60).pdf
3181K

Encl (61).pdf
1080K

No.: Z-28016/195/2017-PMSSY-IV
Government of India
Ministry of Health and Family Welfare
(PMSSY - IV Section)
***

Room No: 745A, Nirman Bhawan, New Delhi

Dated 19-05-2025

To

Executive Director, all new AIIMS

Subject: Engagement of Retired Faculty on contract basis in new AIIMS - reg.

Sir/ Madam,

In partial modification of this Ministry's letter of even no. dated 16.11.2017 (copy enclosed) on the subject cited above, it is conveyed that the remuneration in respect of retired faculties engaged in new AIIMS is required to be fixed in accordance with para 6 of Department of Expenditure's OM dated 09.12.2020 (copy enclosed).

2. The above guidelines may be noted for strict compliance.

3. This issues with the approval of the Competent Authority.

Encl: As above

Yours faithfully,

Digitally signed by
ARUN KUMAR BISWAS
Date: 19-05-2025
12:42:24

(Arun Kumar Biswas)
Under Secretary to the Government of India
Email: ak.biswas57@nic.in

Copy to: Dy. Director (Admin), all new AIIMS

No. Z-28016/195/2017-PMSSY-IV
Government of India
Ministry of Health and Family Welfare
Department of Health and Family Welfare

Nirman Bhawan, New Delhi
Dated the 16th November, 2017

To

1. The Director, AIIMS, Patna, Phulwari Sharif,Patna, BIHAR.
2. The Director, AIIMS, Jodhpur, Basni, Jodhpur, Rajasthan
3. The Director, AIIMS, Rishikesh, Virbhadra Road, Rishikesh. Uttrakhand
4. The Director, AIIMS, Raipur, Tatibandh, G E Road, Raipur. Chhattisgarh.
5. The Director, AIIMS, Bhubaneswar, Sijua, Patrapada, Bhubaneswar, Odisha.
6. The Director, AIIMS, Bhopal, Saket Nagar, Bhopal, Madhya Pradesh.

Subject:- Engagement of Retired Faculty on contract basis in new AIIMS-reg.

Madam/Sir,

The matter regarding engagement of retired Faculty at the level of Professor, Additional Professor and Associate Professor, on contract basis, in new AIIMS, up to the age of 70 years, from Institutes of National Importance (INIs) and Government Medical Colleges (GMCs) has been examined in consultation with Integrated Finance Division (IFD), MoHFW.

2. In this regard, approval of the competent authority is conveyed for engagement of retired Faculty at the level of Professor, Additional Professor and Associate Professor, on contract basis, in new AIIMS, up to the age of 70 years, from Institutes of National Importance (INIs) and Government Medical Colleges (GMCs). The retired Faculty to be taken on contract would be termed as Professor (Consultant); Additional Professor (Consultant); Associate Professor (Consultant). Other details are appended below:

(i) The contractual engagement of retired Faculty would be against vacant regular posts in new AIIMS, and there would be continued attempts for direct recruitment of Faculty by open advertisements.

(ii) The approved lumpsum remuneration for retired Faculty Consultants would be as under:

i) Professor (Consultant) - Rs 2,20,000/-
ii) Additional Professor(Consultant) - Rs 2,00,000/-
iii) Associate Professor (Consultant) - Rs 1,88,000/-

(iii) Retired Faculty Consultants in the event of being provided campus accommodation/ guest house facilities, applicable deductions in respect of such accommodation would be made from the above remuneration, as under:

i) Professor (Consultant) - Rs.24,000/-+applicable licence fee
ii) Additional Professor (Consultant) - Rs.22,000/-+applicable licence fee
iii) Associate Professor (Consultant) - Rs.20,000/-+applicable licence

Contd...

File No. Z-28016/195/2017-PMSSY.IV (Computer No. 3126407)
Generated from eOffice by SARITA, EA(S)-PMSSY, DEO, DOHFW DEPARTMENT on 19/05/2025 12:08 pm

(iv) Participation of Retired Faculty in National Seminars/Conferences would be permissible as per entitlement of regular Faculty. TA/DA on tour, as admissible, as per entitlement against post last held, would be given.

3. The approved Terms and Conditions (ToC) for engagement of Retired Faculty Consultants on contract basis is enclosed herewith.

Yours faithfully,

(P A Mini)
Director
Tel.011-23061288

Encl: As above.

Terms and Conditions (ToC) of Engagement of Retired Faculty Consultant on Contract basis in new AIIMS

The Terms and Conditions of engagement of Retired Faculty Consultant on contract basis in new AIIMS are as follows:

i) The engagement of retired faculty consultant is purely on contract basis for an initial term of two years from the date of joining duty after acceptance of this contract. The term may be extended by another two years or till the attainment of age of 70 years or till the post is filled by regular appointment, whichever is earliest. The period of contract is subject to be reduced or extended at the sole discretion of the Competent Authority in the new AIIMS institute.

ii) The retired faculty consultant will be assigned clinical, teaching and research duties, besides any other work as deemed fit by the Director of the Institute.

iii) The retired faculty consultant will report to the Director of the Institute.

iv) During the period of contract, retired faculty consultant will be paid a consolidated monthly remuneration as indicated in the letter of engagement subject to satisfactory output. His remuneration shall be all inclusive and subject to deduction of tax at source and / or any other statutory deductions to the extent required under the laws.

v) Participation of retired faculty consultant in National Seminars/ Conferences would be permissible as per entitlement of regular Faculty. In case retired faculty consultant is also deputed out of station on official assignment, TA/DA would be paid on tour, as admissible, as per entitlement against post last held immediately before retirement.

vi) Retired Faculty Consultant will be eligible for thirty(30 days) leave in a calendar year, on cumulative basis.

vii) During the period of contract, the engagement is liable to be terminated at any time with a one month notice, without assigning any reason whatsoever. It will be open to the Institute to pay, in lieu of notice, salary for the period by which the notice period falls short. Similarly, the retired faculty consultant may also terminate the contract any time with one month's notice. The termination may be allowed with lesser notice period also provided the retired faculty consultant deposits with the Institute appropriate amount equivalent to the consolidated remuneration of the period by which the notice period falls short, in lieu of the notice period.

viii) Private practice of any kind, including laboratory and consultant practice is prohibited. The retired faculty consultant will not engage himself/herself in any other paid assignment during the validity of this contract.

ix) If at any time, in the opinion of competent authority, which is final in this matter, retired faculty consultant is found non-performing or guilty of any offence, dishonest, disobedience, disorderly behaviour, negligence, indiscipline, absence from duty without permission or any other conduct considered by the competent authority, deterrent to the interest of AIIMS or violation of one or more terms and conditions of this letter, his/her services may be terminated without notice and the competent authority shall be entitled to recover any damages arising out of any act or omission on his/her part, from him/her.

x) Other conditions of service will be as provided under the Rules, Bye laws and Regulations of the Institute and governed by the relevant rules and orders issued by the Government of India.
It may please noted that the retired faculty consultant will be required to conform to the Rules, Bye laws, Regulations, Discipline and Code of Conduct prevailing in the Institute from time to time.

xi) Retired Faculty Consultant will be governed, in respect of any matter relating to the conduct, discipline, in respect of which no provisions have been made in these terms and conditions, the provisions of CCS Conduct Rules 1964 and Central Civil Services Classification Control and Appeal Rules 1965 as amended from time to time.

xii) Retired Faculty Consultant will be at the disposal of the Institute on whole time basis and his/her services may be utilized in any manner required by the Competent Authority of the Institute without any claims for any additional remuneration.

xiii) The Institute will not be responsible for any loss, accident, damages or injury while performing the consultancy assignment including travel.

xiv) Retired Faculty Consultant will not have or acquire during validity of this contract either directly or indirectly any outside interest, in any business or otherwise, which could be in conflict with the interest of Institute as a whole or that would be prejudicial to his/her position. Retired Faculty Consultant will declare any interests in, any commercial concern or companies etc. before joining. Failure to do so will entail termination of his/her contract forthwith without prejudice to the right of this Institute for initiation of legal action against him/her as deemed fit.

xv) Retired Faculty Consultant and his/her family members shall not accept any gifts or presentations, directly or indirectly, whether in the form of money, free possession of goods or other benefits from any person or firm with whom he/she is or likely to be, in contract, by virtue of this contract with whom he/she has or is likely to have dealings. His/her services would be terminated, if found involved in corrupt practices, besides taking action as per rules/law.

xvi) Retired Faculty Consultant will devote his/her whole time and attention exclusively to the duties entrusted to him/her to the best of his/her power,

ability and skill. He/ She will acknowledge that his/her position entails absolute confidentiality and therefore during the continuance of this contract/ arrangement and / or after cessation of this contract for any reasons whatsoever, he/she will not indulge or disclose any information papers and documents in his/her knowledge and custody to any outsider and maintain absolute confidentiality.

xvii) Retired Faculty Consultant is liable to make good any of loss sustained by the Government due to his/her misbehaviour or negligence.

xviii) Retired Faculty Consultant will not engage himself/herself in any other paid assignment during the validity of this contract.

xix) Retired Faculty Consultant will not disclose or divulge or make public or shall personally use for any gain any of the materials, processes, accounts, transactions, dealings, information etc. whether the same may be confined to him/her or may become known to him/her during the course of his/her services or otherwise.

xx) In case Retired Faculty Consultant is employed elsewhere, he/she will bring a letter from his/her present employer stating that his/her resignation has been accepted and he/she is relieved.

xxi) In case any of the above conditions are violated, the appointment shall automatically stand cancelled.

xxii) Upon termination for whatever reasons, Retired Faculty Consultant will forthwith return to Institute all records/documents and papers that are in his/her custody and control, by virtue of his/her engagement and obtain discharge in writing from Institute.

xxiii) Retired Faculty Consultant will not seek or try to secure any other job or employment without previous written sanction/consent of the Institute.

xxiv) There will be periodical monitoring of the performance of the contractual appointee and in the event that his/her performance is found to be unsatisfactory, his/her contract is liable to be terminated and/or his/her payments withheld till satisfactory progress is achieved by him/her.

xxv) This contract shall be governed by the rules, regulations and law of the Government of India.

xxvi) In the event of any conflict regarding terms of appointment, the decision of the Institute shall be final.

****

F. No. 3-25/2020-E.IIIA
Government of India
Ministry of Finance
Department of Expenditure

Dated the 9th December, 2020

Office Memorandum

Subject: Regulation of Remuneration in case of Contract Appointment of Retired Central Government Employees.

The undersigned is directed to say that Ministries/Departments appoint retired Central Government employees on contract basis, including as Consultants on contract basis. However, at present there are no uniform guidelines for regulation of remuneration in such cases.

2. The existing instructions of Department of Personnel and Training, as contained in their Central Civil Services (Fixation of Pay of Re-employed Pensioners) Orders, 1986, as amended from time to time, provide for regulation of pay in case of re-employment. However, the instructions of Department of Personnel & Training as contained in their OM No. 26012/6/2002- Estt (A) dated 9.12.2002 provides that re-employment beyond the age of superannuation of 60 years shall not be permissible. Also, as per their OM No. 3(3)/2016-Estt (Pay II) dated 1.5.2017, the pay plus gross pension on re-employment is not to exceed Rs.2,25,000/-, i.e. Pay Level 17 as applicable to an officer of the level of Secretary to the Government of India.

3. Aforementioned instructions of Department of Personnel & Training on pay fixation in case of re-employment apply only to persons appointed on re-employment. These are not applicable to persons employed on contract basis except where the contract provides otherwise. Accordingly, in cases of appointment of retired Central Government employees on contract basis after the age of superannuation at 60 years, the instructions on pay fixation on re-employment will not directly apply.

4. Department of Personnel & Training has also informed that they are in the process of drafting a Note for Committee of Secretaries (CoS) regarding guidelines for engagement of retired Government servants as Consultant in Government Ministries and Department. In view of this, till Department of Personnel and Training finalizes their guidelines, there is a need to regulate remuneration in such cases of contract appointment of retired Central Government employees on a uniform basis. The matter has, therefore, been considered and it has been decided that regulation of remuneration in case of appointment of retired Central Government employees on contract basis, including as consultants, shall be regulated as provided hereinafter.

5. At the outset, such appointments shall not be made as a matter of practice and must be kept at a bare minimum. Such appointments may be made only in the justified exigencies of the official work where public interest is served by appointment of the retired employee. While making such appointments, adequate functional necessity with clear grounds must be placed before the appointing authority.

6. **Remuneration**

6.1 A fixed monthly amount shall be admissible, arrived at by deducting the basic pension from the pay drawn at the time of retirement. The amount of remuneration so fixed shall remain unchanged for the term of the contract. There will be no annual increment / percentage increase during the contract period.

Example

An employee retired in the Pay Level 13 and the pay at the time of retirement was Rs. 1,55,900. Thus, the basic pension will be Rs. 77,950. If the employee is appointed on contract basis, including as Consultant, the remuneration shall be fixed at Rs.77,950 (1,55,900-77950).

6.2 The basic pension to be deducted from the last pay drawn shall be the pension as fixed at the time of retirement and as such, if the employee has availed of the commuted value of pension, the commuted portion of pension shall also be included in the portion of pension to be deducted. Thus, in the above example, if 40% of pension was commuted, the commuted portion shall be Rs. 31,180 (40% of 77,950) and the pension actually drawn shall be Rs. 46,770. However, the amount of pension to be deducted from the last salary shall be Rs 77,950.

6.3 No Increment and Dearness Allowance shall be allowed during the term of the contract.

7. **Allowances**

7.1 **House Rent Allowances**

No HRA shall be admissible.

7.2 **Transport Allowance**

An appropriate and fixed amount as Transport Allowance for the purpose of commuting between the residence and the place of work shall be allowed not exceeding the rate applicable to the appointee at the time of retirement. The amount so fixed shall remain unchanged during the term of appointment. However, retired employees engaged as consultants may be allowed TA/DA on official tour, if any, as per their entitlement at the time of retirement.

7.3 **Leave of absence**

Paid leave of absence may be allowed at the rate of 1.5 days for each completed month of service. Accumulation of leave beyond a calendar year may not be allowed.

8. **Term of Appointment**

8.1 The term of appointment shall ordinarily be for an initial period not exceeding one year which is extendable by another one year. Beyond two years after the age of superannuation where adequate justification exists, the term may be extended based on a review of the task and the performance of the contract appointee, provided it shall not be extended beyond 5 years after superannuation.

8.2 The consultant shall sign an agreement of confidentiality with the Government of India containing a clause on Ethics and Integrity.

9. **Exemptions**

The terms of appointment provided for in these orders shall not apply to cases and to the extent where the Appointments Committee of Cabinet has allowed special terms OR where special provisions have been allowed with the approval of the Department of Personnel & Training OR Department of Expenditure.

10. These orders shall apply to appointments made in the Central Government and shall be effective from the date of issue of the orders, until further orders or until instructions are issued by DoPT regulating remuneration of retired Government employees on their engagement as consultants. The past cases shall not be reopened in the light of these orders until the normal term of those past cases. Any relaxation of the above will be required to be referred to Department of Expenditure.

(B.K.Manthan)
Deputy Secretary

To,

All the Ministries and Departments of the Government of India as per the standard list.

DDA AIIMS PATNA <dda@aiimspatna.org>

Technical Allowance (Tier-I and II) in respect of Defence Personnel appointed on deputation basis in New AIIMS

3 messages

pmssysection iv <pmssysectioniv@gmail.com> Mon, May 19, 2025 at 12:31 PM
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, drppjoshi@aiimsnagpur.edu.in, Executive Director Raebareli <edaiimsrbl@gmail.com>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, "Sharma, DN" <sharmadn@aiims.edu>, "Dr.Shakti kumar Gupta" <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, madhabananda@gmail.com, sachimohanty@rediffmail.in
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, Rajeev Sen Roy <rajeevsenroy30@gmail.com>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, dda@aiimsrbl.edu.in, "Dy Director Administration AIIMS, Raebareli" <ddaaiimsrbl@gmail.com>, "Dr. Pradip Kumar" <kpradip10@gmail.com>, dda@aiimskalyani.edu.in, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, dda@aiimsbilaspur.edu.in, Mukesh Kumar <mac.prasad@gmail.com>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, aps101982@rediffmail.com, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, Administrative Officer <ao.aiimsmadurai@gmail.com>, T Ngamlien <t.ngamlien@icg.gov.in>, ddaaiimsawantipora1@gmail.com, ":" <Ak.biswas57@nic.in>, Taranjeet Singh <taranjeet.singh@nic.in>, "Mr.SankarGarg Mr.SankarGarg" <sankar.garg@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officers of PMSSY-IV Section at - arvind.thakur@nic.in; ak.biswas57@nic.in; taranjeet.singh@nic.in, sankar.garg@gov.in;
Regards

PMSSY-IV Section
Ministry of Health and Family Welfare

Letter (290).pdf
87K

DDA AIIMS PATNA <dda@aiimspatna.org> Tue, May 20, 2025 at 3:46 PM
To: Amit Kumar Sinha <amit.sinha@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507
[Quoted text hidden]

Letter (290).pdf
87K

Director . <director@aiimspatna.org> Wed, May 28, 2025 at 11:18 AM
To: DDA AIIMS PATNA <dda@aiimspatna.org>

For Compliance.

Regards!
Sd/-
Prof. (Dr.) Saurabh Varshney
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109

---------- Forwarded message ---------
From: **pmssysection iv** <pmssysectioniv@gmail.com>
Date: Mon, May 19, 2025 at 12:31 PM
Subject: Technical Allowance (Tier-I and II) in respect of Defence Personnel appointed on deputation basis in New AIIMS
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, <drppjoshi@aiimsnagpur.edu.in>, Executive Director Raebareli <edaiimsrbl@gmail.com>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, Sharma, DN <sharmadn@aiims.edu>, Dr.Shakti kumar Gupta <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, <madhabananda@gmail.com>, <sachimohanty@rediffmail.in>
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, Rajeev Sen Roy <rajeevsenroy30@gmail.com>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, <dda@aiimsrbl.edu.in>, Dy Director Administration AIIMS, Raebareli <ddaaiimsrbl@gmail.com>, Dr. Pradip Kumar <kpradip10@gmail.com>, <dda@aiimskalyani.edu.in>, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, <dda@aiimsbilaspur.edu.in>, Mukesh Kumar <mac.prasad@gmail.com>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, <aps101982@rediffmail.com>, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, Administrative Officer <ao.aiimsmadurai@gmail.com>, T Ngamlien <t.ngamlien@icg.gov.in>, <ddaaiimsawantipora1@gmail.com>, : <Ak.biswas57@nic.in>, Taranjeet Singh <taranjeet.singh@nic.in>, Mr.SankarGarg Mr.SankarGarg <sankar.garg@gov.in>

[Quoted text hidden]

Letter (290).pdf
87K

Z-28016/246/2015-SSH-Part (2)
8024020
Government of India
Ministry of Health & Family Welfare
PMSSY-IV Section

Nirman Bhawan, New Delhi
Dated the 19.05.2025

To,

Executive Director of all new AIIMS

S u b : Technical Allowance (Tier-I and II) in respect of Defence Personnel appointed on deputation basis in New AIIMS

Madam/Sir,

I am directed to refer to the subject cited above and to say that the matter regarding admissibility of Technical Allowance (Tier-I and II) in respect of Defence Personnel selected on non-technical posts of DDA and FA on deputation basis in New AIIMS was examined in consultation with MoD, and MoD vide its letter dated 27.03.2025 (copy enclosed) has clarified that the Technical Allowance (Tier-I and II) **will not be admissible** in case the officers are appointed against posts which are not actually related to technical and maintenance duties.

2 In view of the above, it is conveyed thatTechnical Allowance (Tier-I and II) is not admissible for Defence Personnel appointed on deputation to new AIIMS on posts which are non-technical in nature.

3. Accordingly, in light of the above clarification you are requested to take necessary action and ensure that the Technical Allowance is not drawn by Defence Personnel appointed on deputation basis in new AIIMS on posts which are non-technical in nature.

Yours faithfully
Digitally signed by
Taranjeet Singh
Date: 19-05-2025
10:47:31
(Taranjeet Singh)
Under Secretary to the Government of India
Tel:011-23061343

Copy to:-

Deputy Director (Administration), of all new AIIMS

DDA AIIMS PATNA <dda@aiimspatna.org>

Extension in the period of deputation tenure beyond the initial period of 3 years in new AIIMS - reg.

2 messages

pmssysection iv <pmssysectioniv@gmail.com> Wed, May 21, 2025 at 3:12 PM
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, drppjoshi@aiimsnagpur.edu.in, Executive Director Raebareli <edaiimsrbl@gmail.com>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, "Sharma, DN" <sharmadn@aiims.edu>, "Dr.Shakti kumar Gupta" <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, madhabananda@gmail.com, sachimohanty@rediffmail.in
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, Rajeev Sen Roy <rajeevsenroy30@gmail.com>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, dda@aiimsrbl.edu.in, "Dy Director Administration AIIMS, Raebareli" <ddaaiimsrbl@gmail.com>, "Dr. Pradip Kumar" <kpradip10@gmail.com>, dda@aiimskalyani.edu.in, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, dda@aiimsbilaspur.edu.in, Mukesh Kumar <mac.prasad@gmail.com>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, aps101982@rediffmail.com, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, Administrative Officer <ao.aiimsmadurai@gmail.com>, T Ngamlien <t.ngamlien@icg.gov.in>, ddaaiimsawantipora1@gmail.com, ":" <Ak.biswas57@nic.in>, Vaishali Vinayak <vaishali.vinayak@gov.in>, Amit Batra <amit.batra@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officers of PMSSY-IV Section at - arvind.thakur@nic.in; ak.biswas57@nic.in; vaishali.vinayak@gov.in; amit.batra@gov.in

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

2 attachments

Letter (304).pdf
90K

Encl (66).pdf
103K

Director . <director@aiimspatna.org> Wed, May 21, 2025 at 3:17 PM
To: DDA AIIMS PATNA <dda@aiimspatna.org>

Sd/-
Prof. (Dr.) Saurabh Varshney
Executive Director

All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109
[Quoted text hidden]

---

2 attachments

Letter (304).pdf
90K

Encl (66).pdf
103K

No. Z-28016/88/2025-PMSSY-IV(8335252)
Government of India
Ministry of Health and Family Welfare
(PMSSY - IV Section)
***

Room No: 745A, Nirman Bhawan, New Delhi

Dated 21-05-2025

To

Executive Director(ED), of all new AIIMS

Subject: Extension in the period of deputation tenure beyond the initial period of 3 years in new AIIMS - reg.

Sir/ Madam,

Reference is invited to this Ministry's letter of even no. dated 15.05.2025 (copy enclosed) on the subject mentioned above.

2. All new AIIMS are requested to submit the details of cases of overstayal, where the officer is continuing on deputation beyond the initial tenure of 3 years without approval of the competent authority. i.e. Secretary(HFW), for consideration by the Ministry, by 31.05.2025 positively.

3. The details to be provided by the institute shall include the following:

i. Copy of the willingness indicated by the officer for extension of deputation tenure.

ii. Copy of NOC provided by Cadre Controlling Authority.

iii. Vigilance status, including details of complaints, if any received against the officer.

iv. Copy of notings of the Institute processed for unilaterally extending the deputation tenure.

v. Copy of the order issued by the Institute for extension of the deputation tenure.

4. This issues with the approval of the Competent Authority.

Encl: As above

Yours faithfully,
Digitally signed by
ARUN KUMAR BISWAS
Date: 21-05-2025
14:54:52
(Arun Kumar Biswas)
Under Secretary to the Government of India
Email: ak.biswas57@nic.in

Copy to: Dy. Director (Admin), all new AIIMS

Z-28015/88/2025-PMSSY-IV(8335252)
Government of India
Ministry of Health & Family Welfare
(PMSSY-IV Section)

Room No. 745-A, Nirman Bhawan, New Delhi
Dated the 15-05-2025

To,

Executive Director (ED), of all new AIIMS

Subject: Extension in the period of deputation tenure beyond the initial period of 03 years in new AIIMS.

Sir/ Madam,

Reference is invited to the 'Consolidated guidelines on deputation/foreign service for Central Government employees' issued by the Department of Personnel and Training vide OM No. DOPT- 1726140763694 dated 28.03.2024. The guidelines provide *inter alia* the following:

> *"8.2 In case where the period of deputation/foreign service prescribed in the RRs of the ex-cadre post is 5 years or less than 5 years, the borrowing Ministry/Department/Organization may grant extension upto the 6th year after obtaining orders of their Secretary (in the Central Government)/ Chief Secretary (in the State Government)/ equivalent officer (in respect of other cases) and for the 7th year with the approval of the Minister of the borrowing Ministry/Department and in respect of other organizations with the approval of the Minister of the borrowing Ministry/Department with which they are administratively concerned.*
>
> ...
>
> ...
>
> *12. The deputationist officer is deemed to have been relieved on the date of expiry of the deputation period unless the competent authority has with requisite approvals, extended the period of deputation, in writing, prior to the date of its expiry. It will be the responsibility of the immediate superior officer to ensure that the deputationist does not overstay. In the event of the officer overstaying for any reason whatsoever, he/she is liable to disciplinary action and other adverse Civil/Service consequences which would include the period of unauthorized overstay not being counted for service for the purpose of pension and that any increment due during the period of unauthorized overstay being deferred with cumulative effect, till the date on which the officer rejoins his parent cadre."*

2. In terms of the extant instructions, the appointments to non-faculty posts in new AIIMS on deputation basis are being made for a period of 03 years. In terms of DoPT's aforesaid OM dated 28.03.2024, extension of deputation tenure upto 6th year requires approval of Secretary (in the Central Government)/Chief Secretary (in the Central Government)/equivalent officer (in respect of other cases). It has been

observed that some new AIIMS have been extending the deputation tenure of various posts beyond the initial approved tenure without obtaining the prior approval of Secretary (HFW). The posts of Chief Executive officer in new AIIMS is being operated at Level 15 of the pay matrix as Executive Director, and thus cannot be equated with the post of Secretary to the Government of India, the level at which the cases for extension in deputation tenure are to be decided in terms of DoPT's aforesaid OM dated 28.03.2024.

3. It is, accordingly, clarified that in compliance with DoPT's aforesaid OM dated 28.03.2024, all cases for extension in deputation tenure in new AIIMS, beyond the initial period 03 years upto 06th year, require prior approval of Secretary (HFW).

4. The instructions contained in para 12 of DoPT's OM dated 28.03.2024 shall apply to unauthorized overstay where the officers are continuing on deputation posts beyond the initial period of 03 years without prior approval of the competent authority.

5. All Executive Directors of AIIMS are advised to comply with the above OM of DoPT in letter and spirit and forward all cases of extension on deputation of officials in AIIMS beyond 3 years for consideration and approval of Secretary HFW.

6. Overstayal of officers in the Institutes beyond the period of deputation without approval of the Competent Authority will be viewed seriously. Any approval for extension of deputation beyond 3 years granted at the level of the Institute is to be treated as null and void.

7. This issues with the approval of the Competent Authority.

Encl(1): OM No. DOPT- 1726140763694 dated 28.03.2024

Yours faithfully
Digitally signed by
ARUN KUMAR BISWAS
Date: 15-05-2025
11:32:50
(Arun Kumar Biswas)
Under Secretary to the Government of India
Tel:011-23061343
ak.biswas57@nic.in

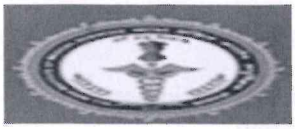
Copy to:

i. Deputy Director(Admin) of all new AIIMS

Copy for information to:

i. PSO to Secretary(HFW)

ii. PPS to JS(PMSSY)



Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Compliance in respect to the Guidance Framework for Cyber Crises Management Plan-reg.

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, Dec 18, 2025 at 10:56 AM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **mn mishra** <mnmishra.mohfw@gmail.com>
Date: Fri, May 24, 2024 at 2:21 PM
Subject: Fwd: Compliance in respect to the Guidance Framework for Cyber Crises Management Plan-reg.
To: DDA AIIMS Rishikesh <dda@aiimsrishikesh.edu.in>, DDA AIIMS Jodhpur <dda@aiimsjodhpur.edu.in>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, Dy Director Administration AIIMS, Raebareli <ddaaiimsrbl@gmail.com>, DDA AIIMS Bhopal <dydir@aiimsbhopal.edu.in>, Deputy Director Administration <dda@aiimsbhubaneswar.edu.in>, <dda@aiimspatna.org>, <dda.aiimsrajkot@gmail.com>, <dda@aiimsnagpur.edu.in>, <dda.aiimsbibinagar@gmail.com>, <ddaaiimsjammu@gmail.com>, <ddamadurai1189@gmail.com>, <dda@aiimsdeoghar.edu.in>, <dda@aiimsmangalagiri.edu.in>, Recruitment Cell AIIMS, Bathinda <recruitmentaiimsbathinda@gmail.com>, <ddaaiimsbilaspur@gmail.com>
Cc: cc: Narendra K Oza <nk.oza@gov.in>, <prasad-upsc@gov.in>, DINESH KUMAR <dinesh.kumar14@nic.in>, ShriRajKumar Under Secretary <raj.kumar28@nic.in>

Sir,
As per trailing mail,Kindly take necessary action.

Regards,
Er.M.N.Mishra
IT Consultant, PMSSY,
MoHFW,Nirman Bhawan,
New Delhi

---------- Forwarded message ---------
From: **Shri Raj Kumar Deputy Secretary** <raj.kumar28@nic.in>
Date: Tue, May 21, 2024 at 2:17 AM
Subject: Fwd: Compliance in respect to the Guidance Framework for Cyber Crises Management Plan-reg.
To: mnmishra mohfw <mnmishra.mohfw@gmail.com>, T Chinsum Naulak <chinsum.n@nic.in>

Raj Kumar
राज कुमार
Deputy Secretary
PMSSY and SNA
Ministry of Health and Family Welfare
Tel. no. 23063178

From: "EHealth Section" <telmed-mohfw@gov.in>
To: asfa-mohfw@nic.in, "pamposh Pokhriayl" <pamposh.pokhriyal@nic.in>, "dr pulkesh" <dr.pulkesh@gov.in>, "Samsul Haque" <samsul.haque@nic.in>, "ROLI SINGH" <asfr-mohfw@gov.in>, "Noorin Bux Khan" <noorinbux@ord.gov.in>, "Manoj Kumar Sinha" <mk.sinha26@nic.in>, "Ms. V Hekali Zhimomi" <zhimomiv@ias.nic.in>, "Aradhana Patnaik" <asmd-mohfw@nic.in>, "Elangbam Robert Singh" <robert.elangbam@gov.in>, "ANKITA MISHRA BUNDELA" <ankita.edu@nic.in>, "Ghulam Mustafa" <ghulam.mustafa@nic.in>, "ARADHANA PATNAIK" <jsadmn-mohfw@gov.in>, "Rajiv Manjhi" <rajiv.manjhi@nic.in>, "Vandana Jain" <vandana.jain@nic.in>, "Vipul Aggarwal" <dr.vipul@nic.in>, "Pradeep Khasnobis" <pradeep.khasnobis@gov.in>, "Rakesh Kumar Maurya" <rakesh.maurya@gov.in>, "Indrani Kaushal" <indrani.k@nic.in>, "Indrani Kaushal" <ea-mohfw@nic.in>, "Dr. K. K. Tripathy" <kk.tripathy@nic.in>, "K Srinidhi" <ksrinidhi.kari@gov.in>, "OMPAL SINGH" <op.singh27@nic.in>, sriram-law@nic.in, "N Sriramasubramanian" <sreram-law@nic.in>, "KAMAL ARORA DS" <kamal.arora@nic.in>, "MCTC CGHS" <mctc@cghs.nic.in>, "Arindam Banerjee" <arindam.banerjee@gov.in>, "Priyanka Gera" <priyanka.gera@gov.in>, "Kiran Gopal" <ed.it@nha.gov.in>, "Vipin Singh" <director.itcm@nha.gov.in>, "Mayank Dhingra" <itcons1.security@nha.gov.in>, "Sushil Pal Gahlaut" <sp.gahlaut@nic.in>, "AMIT KUMAR SHARMA" <amitkumar.sharma@gov.in>, "Archana Verma" <archana.verma68@nic.in>, "Rangoli Pathak" <rv.rangoli@gov.in>, "Dr. Neha Garg" <nehagarg.irs@gov.in>
Cc: "G S Chitra" <gs.chitra@nic.in>, "Phool Chandra Prasad" <prasad-upsc@gov.in>, "Harsh Mangla" <harsh.mangla@ias.nic.in>, "Varsha Singh" <varsha.singh@nic.in>, "Narendra K Oza" <nk.oza@gov.in>, "Nidhi Kesarwani" <nidhikesarwani@nic.in>, "Pawan Kumar" <pawan.kumar13@nic.in>, "ROLI KHARE" <roli.khare@gov.in>, "Sachin Kumar" <sachin.k@nic.in>, "Swarup Dutta" <swarup.dutta@nic.in>, "Kumar Rahul" <kumar.rahul@nic.in>, "eOffice PMU" <eoffice-pmu@nic.in>, "RAJ KUMAR" <rkumar.edu@nic.in>, "Rakesh Kumar" <rk.singh67@nic.in>, "Poonam Meena" <poonam.22@gov.in>, "Sarvajit Kumar" <kumar.sarvajit@nic.in>, "Gopal Aaditya Raghuvanshi" <gopal.aaditya@nic.in>, "Sarita Nair" <sarita.nair@gov.in>, "Shri Raj Kumar Deputy Secretary" <raj.kumar28@nic.in>, "Zuber Ahmed Khan" <us-doj@mha.gov.in>, "C K RAMASWAMY" <ck.rswamy@nic.in>, "ESHITA MONGA" <eshita.monga@gov.in>, "JITENDER SINGH DD(G)" <jitender.singh28@nic.in>, "ABHIJIT CHAKRABORTY" <abhijit.69@gov.in>, "DINESH KUMAR" <dinesh.kumar14@nic.in>, "partha rkshit" <partha.rkshit@gov.in>, "Nikhil Agarwal" <nikhilkr.agarwal@nic.in>, "subha dhandore" <subha.dhandore@nic.in>, "Shalaka Kujur" <shalaka.kujur@nic.in>, "kaustubh 172261 cbdt" <kaustubh.172261.cbdt@nic.in>, "Secretary NMC office" <secyoffice-nmc@nic.in>, "Uttam Kumar" <nicsi-eoffice@gov.in>, "Swarup Dutta" <swarup.dutta@gov.in>, "SUJEET KUMAR" <sujeet.kumar85@nic.in>, "P M NAIR ASSTT" <pm.nair39@nic.in>, "j bansiwal86" <j.bansiwal86@gov.in>, "MONTY KUMAR JHA" <mk.jha91@nic.in>, "Kajal Goel" <kajal.goel@gov.in>
Sent: Tuesday, May 21, 2024 12:20:45 PM
Subject: Compliance in respect to the Guidance Framework for Cyber Crises Management Plan-reg.

Sir/Madam,

Kindly refer attached OM dated 10.05.2024 regarding the subject cited above for your information and necessary action.

Regards
eHealth Section
Ministry of Health & Family welfare
Room No.-213, D-wing, Nirman Bhawan
New Delhi-110011
Tel No.-23062263

2 attachments

OM dated 10-05-2024 (CCMP).pdf
2751K

CCMP.pdf
2332K

T-21016/60/2023-eHealth
Government of India
Ministry of Health and Family Welfare
eHealth section

Nirman
Bhawan, New Delhi
Dated:
10 May, 2024

OFFICE MEMORANDUM

Subject: Compliance in respect to the Guidance Framework for Cyber Crises Management Plan-reg.

The undersigned is directed to refer to the Guidance Framework for Cyber Crises Management Plan Attached at Annexure -A.

2. In this regard, all concerned Divisions/Sections are requested to kindly take necessary action and to circulate same to the respective autonomous bodies/Institutions/Attached offices etc. i.r.o points pertaining to them as per the Annexure-A (copy enclosed).

Yours faithfully,

17/5/24

(Reena Ashish Dash)
Director (e-health)
01123062655

Encl: As above

To,
All Divisions/Sections of MoHFW, through e-office Notice Board.

Copy to:

1. All JS/EA/DDG(Stats.)
2. PPS to Director(e-health)
3. Sr. Tech. Dir., NIC Health

Guidance Framework

for

Cyber Crisis Management Plan

2019

(Not to be put in public domain)

Government of India
Ministry of Electronics and Information Technology(MeitY)
Indian Computer Emergency Response Team(CERT-In)

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Table of Contents

1 Concept of Cyber Crisis Management Plan (CCMP) 4

1.1 Purpose and scope 4

2 Nature of Cyber Crisis and Contingencies 5

2.1 Cyber Security Event, Incident and Crisis 5

2.1.1 Event 5

2.1.2 Cyber Security Incident 6

2.1.3 Cyber Security Crisis 6

2.2 Types of Cyber Security Incidents 6

2.3 Nature of Cyber Crisis and Contingencies 7

2.4 Cyber Crisis, Possible Targets and Impact 7

2.5 Critical Sector Organisations (in case of State Governments/ UTs) / Key Organisations (in case of Central Government Ministries / Departments) 19

3 Building Cyber Security Capabilities 21

3.1 Cyber Security Must Haves 21

3.1.1 Inventory of Devices and Software 22

3.1.2 Controlled Use of Administrative Privileges 22

3.1.3 Secure Configurations for Hardware and Software 22

3.1.4 Malware Defence 23

3.1.5 Vulnerability and Patch Management 23

3.2 Cyber Resilience 24

3.2.1 Principles of resilience 24

3.2.2 Protection and resilience of Organisations' infrastructure 25

3.2.3 Cyber Resilience components & control matrix 26

3.2.4 Objective 27

4 Incident Prevention 28

4.1 Incident Prevention and Precautionary Measures 28

4.2 Deployment of Information Security experts 37

4.3 IT Security Best Practices Compliance-Levels of Assurance 38

5 Cyber Crisis Recognition, Mitigation and Management 39

5.1 Incident Recognition 39

5.2 Cyber Crisis Management – Roles and Responsibilities 41

5.2.1 Crisis Management Group 41

5.2.2 State Level Crisis Management Committee *(Applicable only for State Govts/UTs)* 42

5.2.3 Indian Computer Emergency Response Team (CERT-In) 42

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

5.2.4 National Critical Information Infrastructure Protection Centre (NCIIPC) 43
5.2.5 <Identify other key stakeholder> 43
5.2.6 <Identify the service providers> 43
5.2.7 Private Sector 43
5.2.8 Control Room of the Ministry/State/UT 44
5.2.9 Reporting of Cyber Crisis 44
5.2.10 Response System 44
5.2.11 Contact Information 45
5.3 Incident Response and Mitigation 45
5.4 Media Management 45
6 Post Incident Activity 46
Appendix - I Planning and Preparation for Incident Handling (ISO 27035) 47
Appendix – II Incident Handling Team Structure 49
Appendix – III Incident Response activities during the First Hour 52
Appendix – IV Information Security Management System (ISMS) 63
Appendix – V Important Security Controls for Effective Cyber Security and Continuous Security Policy Compliance 69
Appendix – VI Guidelines on Cyber Crisis Management and Security of Critical Infrastructure. 84
Appendix – VII Sample Business Impact Analysis (BIA) 97
Appendix – VIII IT Contingency Plan template for use by Critical Sector organisations 103
Appendix – IX Points of Action for preparation Cyber Crisis Management Plans 113
Appendix – X Cyber Resilience Control matrix 116
Appendix – XI IT Security best practices Compliance and Assurance – 'Levels of Assurance'. 119
Appendix XII Nature and Severity of cyber crisis 122
Appendix – XIII Control Room Details of CERT-In & Incident Reporting Procedure 132
Incident Reporting Form 135
Annexure-I 139

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

1 Concept of Cyber Crisis Management Plan (CCMP)

1.1 Purpose and scope

This plan discusses types of cyber incidents, policies, actions and responsibilities for a coordinated, approach to prepare for rapid identification, information exchange, response, and remediation to mitigate and recover from malicious cyber related incidents impacting critical business functions and processes of the <*mention name of the organisation/Ministry/State Government/UT Government*>

This plan takes into consideration the crisis that occur due to cyber security incidents and breaches, and presents a broad based approach to deal with such crisis. The approach and methodology of this Cyber Crisis Management plan is derived from the 'Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism' prepared by CERT-In, MeitY, Government of India.

The field of cyber security is technology intensive and new vulnerabilities emerge with progress in technology giving rise to new types of incidents. As such, the plan of response to cyber security incidents need to be updated on regular basis, preferably once in a year.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

2 Nature of Cyber Crisis and Contingencies

This section identifies different types of threats and crises that affect specific targets. Impact of such crisis on respective targets and critical business functions and services of <Mention name of the organisation/Ministry/State Government/UT Government> are identified to determine suitable response and mitigation actions.

While preparing the CCMP the following actions are kept in mind:

a. Identification of all organisational units under the domain of *<mention name of the organisation/Ministry/State Government/UT Government>*
b. Functions and services of the organisational units listed in (a) above
c. Inventory of all Critical Information assets
d. Risk Assessment and risk management (Ref. ISO 27005:2011)
e. Business Impact Analysis (Ref. BIA template at Appendix VII)
f. Contingency plan for IT systems (Ref. Contingency plan template at Appendix VIII)

Cyber crisis has unique features that are different from a physical crisis. In some cases, the severity of cyber crisis is high but confined to individuals or few organisations in a limited area. In other cases, the severity may be low but widely spread to a larger area.

2.1 Cyber Security Event, Incident and Crisis

2.1.1 Event

An event is any observable occurrence in a system or a network like a user connecting to a network file share or browsing a webpage, or even sending an email. Adverse events are those that have a negative consequence that can lead to a disruption of service and has a negative impact to business/ transaction. Examples of such events are system crashes, slow response on system/network, network flooding, high network utilization etc.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

2.1.2 Cyber Security Incident

A security incident is defined as an adverse event in an information system and/or network that pose a threat to computer or network security. In other words, an incident is any event that causes, or may cause a breach of information security in respect of availability, integrity and confidentiality. Examples of such incidents could be unauthorized access to information system, disruption of data, denial of services/availability, misuse of system resources, computer viruses etc. Any violations of organisation's information security policy would also classify as a security incident. A significant cyber incident is a set of conditions in the cyber domain that requires increased national coordination. This increase in national coordination is triggered when the threat level reaches level 3 and beyond (Chapter 5).

2.1.3 Cyber Security Crisis

A situation wherein security characters of information are compromised as a result of failure of an IT system or network of IT systems, due to technical reasons, intentional acts or negligence, leading to consequences that may threaten lives, organisations trust, national security and public confidence. All cyber security crises are cyber security incidents, however, all cyber security incidents are not cyber security crises but may lead to crisis situations if not attended to in a timely manner.

2.2 Types of Cyber Security Incidents

Any real or suspected adverse event in relation to the security of computer systems or computer networks can be termed as a logical security breach. In other words, a logical security incident can be defined as network or host activity that potentially threatens the security of computer systems. Examples of such incidents could include activity such as:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

- Unwanted disruption or denial of service
- The unauthorized use of a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

2.3 Nature of Cyber Crisis and Contingencies

This section identifies different types of threats and crises that affect specific targets. Impact of such crisis on respective targets and critical business functions and services of *<mention name of the organisation/Ministry/State Government/UT Government>* are identified to determine suitable response and mitigation actions.

While preparing the CCMP the following actions are kept in mind:

a. Identification of all organisational units under the domain of *<mention name of the organisation/Ministry/State Government/UT Government>*
b. Functions and services of the organisational units listed in (a) above
c. Inventory of all Critical Information assets
d. Risk Assessment and risk management (Ref. ISO 27005:2011)
e. Business Impact Analysis (Ref. BIA template at Appendix VII)
f. Contingency plan for IT systems (Ref. Contingency plan template at Appendix VIII)

Cyber crisis has unique features that are different from a physical crisis. In some cases, the severity of cyber crisis is high but confined to individuals or few organisations in a limited area. In other cases the severity may be low but widely spread to a larger area.

2.4 Cyber Crisis, Possible Targets and Impact

Table 2.1 provides a snapshot of nature of cyber security incidents which include attempts (either failed or successful) that can trigger a crisis at individual / organisation, multiple organisations or state level.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Table 2.1: Nature of Cyber Crisis, Possible Targets and Impact

Type of Cyber Crisis	Possible Targets	Related impact
1. Targeted Scanning, Probing and Reconnaissance of Networks and IT Infrastructure	• Sensitive Government and Critical Information infrastructure • Infrastructure at Data Centres and Network Operation Centres ▪ Routers, Switches, Database and DNS Servers ▪ Web portals	• Pre-cursor to hacking and focused attack leading to cyber crisis • Total/partial disruption of e-Governance, Public and Banking services
2. Large scale defacement and semantic attacks on websites • A website defacement is when a Defacer breaks into a web server and alters the contents of the hosted website • Attackers change the content of a web page subtly, so that the alteration is not immediately apparent. As a result, false information is disseminated	• High profile national websites such as President, Prime Minister, Parliament, India Portal, Government Information Dissemination websites of Ministries, Public utility services such as Water supply, Police and commercial organisations etc. • Key economic transaction websites such as banks/Financial Institutions (FI), Insurance, online transactions etc.	• Huge national embarrassment, loss of image, reputation etc. • Total/partial disruption of services/activities • Dissemination of false/misleading information • Monetary loss, damage to reputation, loss of image etc.
3. Malicious Code attacks (virus/worm/ /Trojans/Botnets) • Malicious code or malware is software designed to infiltrate or damage a computer system without the owner's informed	• Large & key national data bases such as tax information network, citizen data base, plan information, passports, reservations, Hospital	• Hanging of Computer systems • Partial or No response from Computer system • Total/partial corruption of data bases

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

consent. Malicious code is hostile, intrusive, or annoying software or program code. Commonly known malware are virus, worms, trojans, Ransomware, Cryptominer, spyware, adware and Bots	Information System etc. • Private users (home/corporate organisations)	• Total/partial break down of data access services • Monetary loss, damage to reputation, loss of image etc
3.1 Malware affecting ICS systems • Sophisticated malware such as Stuxnet / Industroyer / targeting Industrial Control Systems that are part of networks separated through 'airgap' from regular Internet facing networks	• Supervisory Control and Data Acquisition systems (SCADA) and Centralized as well as distributed control systems of power, petroleum, transport, air traffic control, refineries, fertilizers etc and all process industries	• Data Theft, Identity theft and possible espionage • Total/partial disruption of services/activities in one or more critical sectors such as energy, transport, telecommunications, emergency services etc
3.2 Malware affecting Mobile devices Malicious code and malicious applications (apps) affecting operating systems/platforms used for mobile devices such as Symbian, Android, iOS, Windows Mobile etc.	• Mobile devices using affected Operating System and connected Computer systems	• Unauthorized disclosure of user's data and contact details
3.3 Malware affecting IoT		

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

devices Compromised IoT devices, such as cameras, routers, DVRs, wearables, IoT and other embedded technologies, infected with malware like Mirai	• Sensitive Government and Critical Information infrastructure • Private users (home/corporate organisations)	• Total/partial disruption of services/activities in one or more critical sectors such as energy, transport, telecommunications, emergency services etc • Data Theft, possible espionage
4. Attacks on Financial Sectors and Digital payment ecosystem	• Digital Payment instruments • IT infrastructure of Financial Institutions, depositors, insurance, stock exchange • SWIFT network, ATM switch	• Financial and Customer Data breach • Financial frauds • Decline in User trust and confidence in digital ecosystem • Loss of reputation
5. Large scale SPAM attacks Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. SPAM mails may also contain virus, worm and other types of malicious software and are used to infect Information Technology systems. As a result, spamming could disrupt e-mail services, messaging systems and mobile phone communications.	• ISP networks • Large corporate networks • Key Govt. networks	• Significant slow down in network performance • Total/partial disruption of E-mail communication services • Severe drain on network resources. • Significant reduction in access to critical network services. • Increased possibility of virus/worm infection
6. Identity Theft Attack		

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Large scale spoofing • Spoofing is an attack aimed at 'Identity theft' o Spoofing is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage	• High profile users in Government, Corporate and key economic installations	• Increased possibility of identity theft and root privileges compromise leading to penetration into sensitive IT systems and Databases • Loss of sensitive data, monetary loss and loss of image.
• **Social Engineering** Art of manipulating people into performing disclosure actions or divulging confidential information • **Phishing attacks** Phishing is an attack aimed at stealing the 'sensitive personal data' that can lead to committing online economic frauds. Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication • **Vishing attacks** Vishing is a combination of 'voice'	• Individual users such as senior executives & officials, celebrities • Network/System/Database Administrators • Users of Banks/FIs, large e-Commerce organisations, key e-Governance entities etc. • Key Government organisations and Government service providers	• Loss of sensitive personal data, monetary loss and loss of image and trust • Financial frauds • Loss of user credentials • Monetary loss to citizens

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

and 'phishing'. It is the practice of using social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward. It exploits the trust in landline telephone services and uses VoIP to trick the user. • **SMSihing attacks** These are phishing attacks launched through SMS service via Mobile phones.		
7. Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks • DoS is an attempt to make a computer resource unavailable to its intended users • A distributed denial of service attack (DDoS) occurs when multiple compromised computer systems flood the communication link (called bandwidth) or resources of a targeted system. • DDoS attacks are launched through a Botnet which is a	• Public utility services • Fire • Water supply • Hospitals/ Ambulance • Police • Transport • Mission critical systems • Supervisory Control and Data Acquisition (SCADA) System • Web-based key economic targets such as Banks/FIs, Insurance, stock exchange, online reservations etc • Government Organisations and Web-based key economic targets	• Total/partial disruption of services for prolonged periods • Failed/aborted missions • Possible damage to life and/or property • Total/partial disruption of services for prolonged periods

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

network of compromised computer systems called 'Bots'. • Reflection based Distributed Denial of Service (RDDoS) Attack		• Monetary loss, damage to reputation, loss of image etc
8. Domain Name Server (DNS) attacks • DNS Hijacking refers to modification of DNS records with the intention of redirecting the victim to malicious domains/IPs. • NXDOMAIN attacks are performed by flooding DNS servers with queries for invalid or non-existent domains therefore eating up the valuable resources and polluting DNS server cache with NXDOMAIN results. • DNS Cache poisoning involves corrupting the DNS server's cache with fake values causing the name server to return an incorrect results. This may result in traffic being diverted to the malicious systems.	• Country level domain registry systems (NIXI ".IN" registry) • International gateway or ISP/ large corporate server systems • E-commerce • Business and banking applications • Individual users/ home routers • E-governance • Government organisations	• Total/partial disruption of '.in' registry services • Possible damage of/inaccessibility to domain registry database or resolution services • Illegal diversion of Internet and mail traffic to some other countries • Total/partial disruption of internet traffic nationally/internationally • Total/partial break down of on line economic activities • Monetary loss, damage to reputation, loss of image etc
9. Application Level Attacks Exploitation of inherent	• e-Governance • e-Commerce	• Data manipulation which may result in huge economic fallouts including monetary as

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

vulnerabilities in the code of application software such as web/mail/databases	• Business and Banking Applications	well as business loss • Disruption of services • Loss of sensitive data and loss of image & trust
10. Attacks on Trusted infrastructure Trust infrastructure components such as Digital certificates and cryptographic keys are used at various levels of cyber space ranging from products, applications and networks. Compromise of infrastructure of Certifying authority or key management systems of product/application owners may result in breakdown of trust of users and misuse of authentication mechanisms		
(i) Denial of Service attacks	• SSL Servers	• Blocking of handshaking resulting in disruption of financial and authentication services
(ii) Rogue certificates	• Certifying Authorities • Authentication infrastructures • Secure Communication Protocols and systems • Public Key Infrastructure	• Large scale Man-in-the-middle attacks resulting in disclosure sensitive data and user information • Redirection of users to fake websites with dubious authentication • Signing malicious code to make it appear as legitimate • Large scale cyber espionage

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

11. Compound attacks • By combining different attack methods, hackers could launch an even more destructive attack. The Compound attacks magnify the destructiveness of a physical attack by launching coordinated cyber attack.	• Public utility services • Fire • Water supply • Hospitals/Ambulance • Police • Transport • Web based economic targets • Large & key national & economic databases • Mission Critical systems • International gateway/ISPs	• Total/partial disruption of services/activities • Significant slowdown in disaster/emergency response capabilities that can magnify the impact of a physical attack • Huge economic fallouts including monetary as well as business loss • Damage to reputation, loss of image etc.
12. Router level attacks • Routers are the traffic controllers of the Internet to ensure the flow of information (data packets) from source to destination. Routing disruption could lead to massive routing errors resulting in disruption of Internet communication	• Sensitive Government and Critical Information Infrastructure. • Gateway/ISP routers • Routers of large & key economic targets such as bank/FI networks, corporate networks etc. • ADSL/Wi-Fi Routers used by small offices/home users • ISP networks • Large Corporate Networks • Web based economic targets • E-Commerce • Social media websites • Business and Banking applications	• Total/partial disruption of internet traffic nationally/internationally • Total/partial break down of online economic activities • Huge economic fallouts including monetary as well as business loss • Total/partial break down of online economic activities • Huge economic fallouts including monetary as well as business loss • Possession of Router's control by attackers and re-redirection to malicious websites through rogue DNS Server entries for conducting malicious activities

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

• **Border Gateway Protocol (BGP) attacks** BGP is a primary protocol used to route traffic between different networks, known as Autonomous Systems (AS), across the Internet. It works by exchanging routing and reachability information among different AS. BGP route manipulation: A router in the network announces a spurious route which upon propagating prevents traffic from reaching the intended destination. This can occur due to router misconfigurations (intentional / unintentional) or compromised router. BGP route hijacking (prefix hijacking): The attacker announces the more specific prefixes of intended target network to reroute traffic through itself. Once successful, the hijacker could then perform Man-in-the-middle attacks, eavesdropping, modify or block the traffic. BGP Denial of Service (DoS): A compromised router in the network sends unexpected or undesirable BGP traffic to another router. The target router stops processing valid BGP traffic due to		• Illegal diversion of internet traffic • Monetary loss, damage to reputation, loss of image, etc. • Total/partial breakdown of online economic activities. • Loss of sensitive personal data. • Total/partial disruption of internet traffic nationally/ internationally

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

excessive resource consumption.		
13. High Energy Radio Frequency Attacks Use of physical devices like Antennas to direct focused beam which can be modulated from a distance to cause RF jamming of communication systems including Wireless networks leading to attacks such as Denial of Service	• Wireless Networks ▪ Wi-Fi ▪ Wi-MAX • Mobile Networks • Satellite Network Communication Systems	• Disturbances or total disruption in the Wireless, Mobile and Satellite Networks • Appliances like, phones, Bluetooth and Microwave devices etc, • Some RF Jamming tools may use very high energy sufficient to even break down the electronics and make it to malfunction totally.
14. Cyber Espionage and Advanced Persistent Threats Targeted attack resulting in compromise of computer systems through social engineering techniques and specially crafted malware. The data from compromised system is siphoned off to remote locations. Common channel of attacks include spoofed/compromised email accounts of key officials, social networking sites and drive-by-download through watering hole websites.	• Sensitive Government Organisations • Defence • Corporate	• Disclosure of sensitive information • Data theft • Compromise of critical internal systems
15. Client-Side attacks Attacks on client side		

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

vulnerable software applications like MS office applications, Adobe Acrobat reader, JAVA, Browsers Plugins, etc usually via Sophisticated attack tool kits with various exploits available for compromising/rooting the client system.	• Individual users.	• Data Leakage. • User system as bot or launch pad for launching further attacks.
16. Attacks using Social Network Sites (SNS) Attacks targeting Social networking platform for various malicious activities such as identity theft, fake social accounts, fake news, misinformation, command & control for Botnets, drive-by-download etc.	• Individual users such as senior executives & officials, celebrities • Corporates • Political leaders	• Loss of sensitive personal data, loss of image and trust. • Malware distribution.
17. Hybrid Threats & Influencing Hybrid Threats are mixture of coercive and subversive activities which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. Cyber vector can be exploited by adversaries to influence the target. Threats such as Election interferences, hacktivism in electoral campaign,	• Sensitive Government Organisations / officers • nation • Political parties & leaders • States/UTs • Elections	• Election Interferences • Attempts to influence politics and elections • Fake news • Opinion shaping • Disinformation campaigns • Online Radicalization • Manipulating human Psychology

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

opinion shaping, misinformation can be launched by adversaries against the vulnerable nation, state or population		
18. Vendor / Supply chain risk / attack Attacker infiltrates through a outside partner or provider with access to organisations system / data or modifying the product deliberately with malicious backdoor. ex. Includes Trojan, hardware manipulation and software supply chain	• Government Organisations • Critical Sector organisations • Corporate sector	• Disclosure of sensitive information • Cyber espionage • Attack on critical infrastructure • Advanced persistent threats
19. Threats due to Emerging Technologies(Iot, Big Data, Artificial Intelligence) Attacker can make use of the system / data / Compute power / components deliberately with malicious backdoor to attack organisational network	• Government Organisations • Critical Sector organisations • Corporate sector • Cloud Service Providers	• Cyber espionage • Attack on critical infrastructure • Disclosure of sensitive information

2.5 Critical Sector Organisations (in case of State Governments/ UTs) / Key Organisations (in case of Central Government Ministries / Departments)

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Focused cyber-attacks on infrastructure of one or more critical sectors/key organisations, either individually or simultaneously, may result in significant/complete breakdown of supplies or services essential to the life of the citizens including but not limited to financial, Government, law enforcement, transport, energy or communication. These events may lead to national crisis.

The following key sectors/key organisations have been identified:

<organisation1>

<Organisation 2> and .....

These sectors/organisations would include both public and private organisations. This list may be revised from time to time.

3 Building Cyber Security Capabilities

3.1 Cyber Security Must Haves

All organisations should develop culture of cyber security among themselves in every aspect of their functionality. The Cyber Security Must Haves indicates the basic cyber security fundamentals applicable to all the organisations. By deploying these Must Haves, organisations can defend against the most common form of basic cyber-attacks originating from the Internet. The defences identified through these Must Haves deal with reducing the initial attack surface.

These Baseline requirements for cyber security helps organisations to select as a starting point for implementing cyber security program and provides opportunity to benchmark against minimum set of cyber security controls. Minimum set of cyber security controls can be used by organisations as a starting point for journey towards implementing full-fledge cyber security framework.

The figure given below illustrates the 5 Cyber Security Must Haves:



Figure: Cyber Security Must Haves

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

3.1.1 Inventory of Devices and Software

Inventory of Hardware & Software: Create and manage inventory of all hardware and software available on the organisation's network. The inventory of devices and software will help in identifying what needs to be secured and also help in ensuring proper management of the access control.

To accomplish this, organisations needs to maintain an asset inventory of all systems & software connected to the network, preferably deploying an automated asset inventory system to gather the data. The idea behind this control is that we can't protect what we don't know we have and therefore, having an accurate asset inventory is always the first step in securing the organisation against cyber-attacks.

Organisations that do not have complete hardware & software inventories are unable to find unauthorized or vulnerable hardware & software.

3.1.2 Controlled Use of Administrative Privileges

The administrative privileges must be restricted on software, operating systems, devices and network. Mechanism to track and log administrative privileged actions should be maintained. Access to the resources should only be provided on need to know basis.

If administrative privileges are loosely and widely distributed, the attacker has a much easier time gaining full control of the servers & workstations, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges.

Limiting exposure to administrative accounts will reduce the likelihood that an attacker can grab highest privilege in the network.

3.1.3 Secure Configurations for Hardware and Software

Implement and manage secure configuration of hardware and software installed within network. Implement strict configuration rules and change control/approval process. Patching and updates of firmware and software must be ensured. Secure configuration control reduces the attack surface by only operating

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

services and functionalities which are required by organisations in secure fashion. Change management process should be implemented by the organisation, for any required change in the configuration of hardware & software.

Default configurations for hardware and software are normally geared toward ease-of-deployment and not toward security. Open ports and services, default accounts or passwords, vulnerable protocols, pre-installed & unnecessary software are exploitable in their default state. Also, changes in configuration of hardware & software may be performed without any proper change control system which could make system vulnerable to the cyber attacks.

Secure configuration of hardware & software will shrink the attack surface by securing the access to assets in the network by only allowing what is necessary and removing/blocking unnecessary ports & services.

3.1.4 Malware Defence

Malwares are one of the biggest nuisances. Multiple solutions to detect and counter spreading & execution of malware should be deployed in organisations network. Controls for malicious code prevention & detection can be deployed at perimeter security devices, email servers, end-point devices, laptops and servers.

Malware is a broad term that refers to a variety of malicious programs. Malware program contains some lines of code that execute the desired task of attacker when interact with victim system. Some of malware does not require any user interaction. They work as a standalone program. Commonly malwares are adware, bots, bugs, rootkits, spyware, ransomware, rootkits, key loggers, Trojan horses, viruses, and worms.

Organisation should have awareness about malwares, its malicious activities, its impact and should implement the controls to stay safe.

3.1.5 Vulnerability and Patch Management

Based on the cybersecurity alerts, disclosures of vulnerabilities & released exploits, organisations should implement vulnerability and patch management program for ICT environment and take the suitable action at the earliest.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Cybercriminals are exploiting unpatched vulnerabilities in operating systems and common applications, including client side applications such as Java, Adobe, browsers, Office utilities and more. An unpatched vulnerable system is an easy opportunity for attackers to compromise the infrastructure of the organisation.

Vulnerability management is a continuous and pro-active control, it includes identifying vulnerabilities, mitigating vulnerabilities and patching the vulnerabilities.

3.2 Cyber Resilience

Cyber resilience is defined as ability of organisation or business process to anticipate, withstand cyber-attacks and the capability to contain, recover rapidly and evolve to improved capabilities from any disruptive impact of such cyber-attacks.

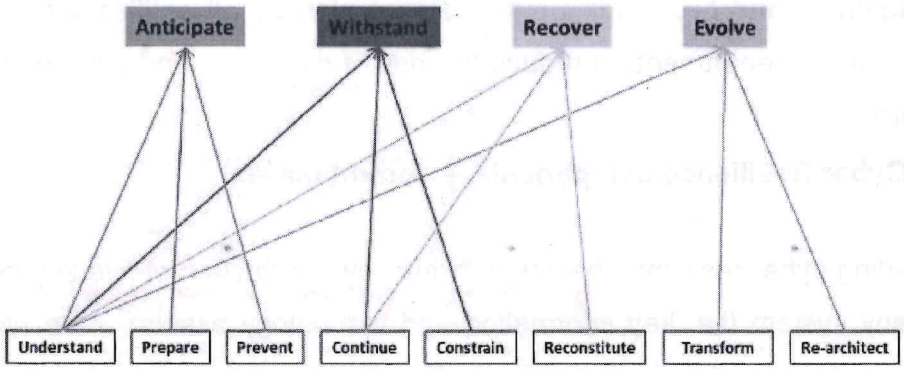
Resilience can be defined in various ways depending upon the area of application or the type of sector under consideration. Common aspects include preparing for, preventing, or otherwise resisting an adverse event; absorbing, withstanding, or maintaining essential functions in the face of the event; recovering from the event; and adapting to (changing processes, systems, or training based on) the event, its consequences, and its implications for the future

3.2.1 Principles of resilience

1. Anticipation, Protection and detection, including vulnerabilities, of cyber infrastructure & systems in organisations to understand, prepare and prevent cyber attacks
2. Withstanding and Localize containment of crisis and isolate trusted systems from untrusted systems to continue essential business operations in the event of cyber attacks
3. Dynamic & reliable automated recovery of crisis impacted systems to restore maximum continuity and operations by following predefined resilience rating or degree of confidence for each of system components and evolving to improved capabilities by making changes to existing processes or workflows and updating / modifying the threat model.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

At a conceptual level, the goals and principles can be shown as in the following diagram:



Cyber resiliency goals and principles

3.2.2 Protection and resilience of Organisations' infrastructure

An organisation need to work towards following to build cyber resiliency:

- Identification of key information and technology assets that support the services of that organisation
- Implementation of controls to protect those assets from cyber attack
- Implementation of controls to sustain the ability of those assets to operate under disruptive events and recover rapidly from disruption.
- Development of processes to maintain and repeatedly carry out the protection and recovery activities.
- Development of appropriate measures to drive these activities.
- To develop a plan for protection of organisation Infrastructure and its integration with business plan and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, cyber crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.
- To closely interact with 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) by providing it the necessary and timely information.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

- To ensure identification, prioritisation, assessment, remediation, and protection of organisation infrastructure and key resources based on the plan for organisation Information Infrastructure.
- To ensure compliance to global security best practices, business continuity management and cyber crisis management plan by all entities within domain of organisation/ department, to reduce the risk of disruption and improve the security posture.

3.2.3 Cyber Resilience components & control matrix

Building cyber resilience begins with effective protection of five key components within any system (i.e. key information and technology assets) – the user identity, system processes, data and hardware & software platform along with network of connections between systems. These components are defined as follows:

Identity: The representation of a user or organisation within a system.

System Processes: The actual programs running within the system that may be executing on behalf of user or at root level within the operating system.

Hardware & Software Platform: Typically, this will be a physical manifestation of the system as hardware and software, but it may also be a virtualized platform residing on a cloud infrastructure or in the data centre. The information security management system (ISMS) Risk Assessment Methodology and Procedures & controls for State Data Centre based on ISO 27001:2005 may be referred at http://meity.gov.in/content/policy-guidelines-state-data-centre-sdc.

Data: The data either physically stored or held in memory within the system.

Network: The communication link between systems and all the protocols for establishing and securing that communication. Commonly, the gateways on the network act as enforced barriers to communication that may act as a boundary or filter to prevent some communications while enabling others such as network firewall.

Achieving cyber resilience is about understanding the sensitivity and interdependency of critical assets and selecting appropriate technical controls for protection, detection, containment and recovery from cyber disruptive activities and

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

assigning resilience rating for each system component by the organisation depending on the services provided by them and their respective Service level Agreements (SLA). A matrix, showing relation between each of the components within system and their mapping to these controls, may be referred at **"Appendix X"**

Cyber Security Exercises

Cyber security mock exercises are to be conducted periodically to enable organisations under nodal Ministry of Central Government/State Government/UT Government to assess their preparedness and resilience in dealing with cyber crisis. Cyber security exercises conducted with the help of CERT-In or sectoral CERT or state CERT or nodal Ministry as may be applicable shall help organisations to learn how to anticipate threats, protect their infrastructure and platform, detect incidents, withstand impacts, recover from attacks and improve their security posture.

3.2.4 Objective

- To enable the participant organisations to assess their ability and preparedness to deal with cyber crisis situations.
- To enable participating organisations to secure their IT networks & systems and resist cyber-attacks by way of effective implementation of Information Security Management System (ISMS) and Sectoral Cyber Crisis Management Plans
- To detect cyber-attacks and determine appropriate response, mitigation and recovery actions

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

4 Incident Prevention

4.1 Incident Prevention and Precautionary Measures

The organisations/Units within the domain of *<mention name of the organisation/Ministry/State Government/UT Government>* should implement the following as precautionary measures to prevent cyber security incidents:

Table 5.1: Prevention and Precautionary Measures

Nomination of Chief Information Security Officers	Nominate Chief Information Security Officers to coordinate the security related issues/implementation within the organisation as well as coordination and interface with CERT-In and *<mention name of the nodal Ministry of Central Government/State Government/UT Government>*.
Information Security Policy and Implementation of Best Practices	Every organisation should formulate Information Security Policy and identify appropriate information security management practices keeping in view their business needs. The identified practices should be implemented. The critical sectors should necessarily implement Information Security Management System (ISMS) Best Practices as per ISO 27001. The following steps should be taken into account while implementing the ISMS. • The Information Security Policy should clearly identify the three components namely process, technology and mitigation of incidents. • Undertake comprehensive Risk Assessment of the Information Technology/Network assets. • Implement appropriate security control measures such as those defined in the ISO 27001 which include Service Level Agreements with various service providers.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

	Steps need to be taken for ISMS implementation are summarized in **Appendix IV.** Where considered necessary, assistance of experts may be taken.
Business Continuity Plan (BCP)	Define Contingency Plan (Business Continuity Plan) to counteract interruptions to business operations/activities and protect critical operations/business processes from effect of major disaster.
Disaster Recovery Plan (DRP)	Establish Disaster Recovery (DR) Plans with adequate redundancy to take over the operation in case of the need.
Security of Information Infrastructure , Network & Applications	Organisations and enterprises should secure the entire IT infrastructure including the network by implementing appropriate hardening measures. Guidelines on "important controls for Effective Cyber Security and Continuous Security Policy Compliance" are given in **Appendix V**. Security devices may be installed at all levels. Servers, Local Area Network (LAN) and Wide Area Network (WAN) infrastructure should be secured by installing appropriate perimeter security devices such as firewalls, Intrusion Prevention System and anti-virus system. Configuration of these security devices should be checked at the time of installation as well as at the time of significant changes for the needed functionalities and security features. • The security mechanism should include appropriate devices and methods to log and monitor the events to detect network scanning, probing and Reconnaissance, flooding attempts on the IT infrastructure. These attempts should be regularly

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

272

	reviewed and analysed for initiating necessary preventive measures. • The remote monitoring and maintenance of the security devices should be strictly restricted to authorized persons only. • The software at network, system and application level should be regularly upgraded by applying/installing upgrades and updates. Application Security Best practices includes: • Implementation of application security controls for both web and mobile applications • Secure application development should be enhanced by applying security checkpoints and techniques at early stages of development as well as throughout the software development life cycle(SDLC). Special emphasis should be applied to the coding phase of development. Security mechanisms that should be used include, threat modeling, risk analysis, static analysis, digital signature, among others. • Comprehensive security assessments of application should be performed before final deployment of application, and after any major changes or upgrades to the system. • Application design and development should ensure compliance to policy and regulation as applicable.
Network Traffic Scanning	The network traffic scanning technique provides visibility into the state of the network and identifies deviations from baselines that may indicate abnormal or suspicious behaviour. The traffic patterns provides leads on the

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

	targeted ports such as 80, 25, 23 which gives leads to the attack targeted on the services like 'http', 'smtp', 'ftp' or spread of malicious code like 'Bots'. For example, if it is observed that suddenly there is rise on the port 25, associated with e-mail service; this may indicate that e-mail based worm is spreading at a high speed. A sudden traffic rise on the IRC ports may indicate surge in the 'Botnet activity'. The network traffic flows thus gives the exact portrait of the communications happening on the network, irrespective of their state whether a normal or an anomaly. Majority of attacks such as Distributed Denial of Service (DDoS), Worm, Spyware, Botnet detection, malicious scan of any nature etc. at the organisation level could thus be detected by analyzing network flow-data traffic. Industry solutions are available to collect and analyze network flow traffic on the gateway routers and switches. Network flow data DO NOT contain any content data and is totally non-intrusive on the network. The organisations may use network flow data for security analysis to detect attacks onto the networks.
Isolation of critical networks	The critical sector organisations, Defence and sensitive organisations use separate physical networks for operations of critical infrastructure and performing their functions. The critical networks should be isolated from other production networks connected over intranet/Internet. At no point of time the gap between critical network and production network over intranet/internet be compromised. No transfer of data from a intranet/internet based network to a critical network or vice versa be allowed. In case required, it should be under strict control and thoroughly screened. There are malicious codes specifically designed

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

	to target critical infrastructure systems by means of spreading through systems connected over internet. Risk assessment and regular monitoring of critical networks is essential for security of critical infrastructure
Implementation of Security Guidelines issued by nodal Ministries and agencies like CERT-In	Organisations should implement Security Guidelines and advisories both with respect to cyber and physical security issued by respective nodal Ministry and CERT-In from time to time.
Vendor Risk Management (VRM)	Vendor risk management (VRM) is a comprehensive plan for identifying and decreasing potential uncertainties and legal liabilities regarding the hiring of 3rd party vendors for information technology (IT) products and services. The use of third-party vendors presents several other risks, the most prominent of which are legal, operational, and reputational. • Proper planning and due diligence need to be taken for vendor risk identification and mitigation. • A robust vendor governance program to be developed to assess critical, high, moderate, and low risk vendors through surveys and assessments. • Vendor performance need to be monitored on regular basis to be continually aware of a vendor's capability to comply with contractual obligations. Vendor KPIs and KRIs should be clearly defined in line with applicable laws, regulations, and standards. • The organisational hierarchy involved in vendor governance need to be defined.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Supply Chain Risk Management	Supply chain risk management is the implementation of to manage both every day and exceptional risks along the supply chain which typically involves four processes: identification, assessment, controlling, and monitoring of supply-chain risks. The best practices to manage supply chain risks are: • Include security requirements in every RFP and contract. • "Right to Audit" on vendor/supplier should be reserved by the organisation and same should be included in the RFP/Contract. • Trusted source during supply, operation and maintenance phase for products and services need to be ensured • The cyber security posture of supplier organisation need to be ensured • After finalization of work contract, involvement of vendor should be there on-site to address any vulnerabilities and security gaps in the supplied products / services. • Secure Software Lifecycle Development Programs and training for all engineers in the life cycle should be organized. • Rigorous controls on access by service vendors should be imposed through proper authorization. • Legacy support for end-of-life products and platforms
Manpower engaged in cyber security activities	**Screening and background checks** Background verification checks on all employees engaged in implementing and monitoring cyber security and cyber crisis management plan, contractors, and third party users should be carried out in accordance with

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

	relevant laws, regulations and ethics, and proportional to the requirements of task and responsibilities, the classification of the information to be accessed, and the perceived risks. Verification checks should take into account all relevant privacy, protection of personal data and/or employment based legislation, and should, where permitted, include the following: a) availability of satisfactory character references, e.g. one business and one personal; b) a check (for completeness and accuracy) of the applicant's curriculum vitae; c) confirmation of claimed academic and professional qualifications; d) independent identity check (passport or similar document); e) more detailed checks, such as credit checks or checks of criminal records. Information security management practices based on ISO 27001 standard provide guidance with regard to screening and background checks in respect of employees and other personnel. The organisation may consider following ISO 27001 best practices. **Roles and responsibilities** Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organisation's information security policy.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

	Security roles and responsibilities should include the requirement to: a) implement and act in accordance with the organisation's information security policies; b) protect assets from unauthorized access, disclosure, modification, destruction or interference; c) execute particular security processes or activities; d) ensure responsibility is assigned to the individual for actions taken; e) report security events or potential events or other security risks to the organisation. Security roles and responsibilities should be defined and clearly communicated to job candidates during the pre-employment process. Job descriptions can be used to document security roles and responsibilities. Security roles and responsibilities for individuals not engaged via the organisation's employment process, e.g. engaged via a third party organisation, should also be clearly defined and communicated. *Incident response matrix in Appendix III of this document indicate the roles and responsibilities of various personnel engaged in incident response activities.*
Audit and Assurance	• Organisations should undertake comprehensive security audit of the entire IT infrastructure networks and applications by independent auditing organisations to discover the gaps with respect to

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

	best security practices and take appropriate corrective actions. A panel of IT security auditing organisations who provide IT security audit is available on CERT-In website www.cert-in.org.in. • The audit of the system should be undertaken at least once in a year and also as and when any significant addition or alteration in respect of hardware, software, network resources, policies and configurations of systems and sub systems are affected. • Following the audit, compliance with the security policy should be documented in the annual report.
Security Training and Awareness	All employees of the organisation and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function. Awareness training should commence with a formal induction process designed to introduce the organisation's security policies and expectations before access to information or services is granted. Ongoing training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. • Latest Technologies and threats • Implementation of Security Policy • Physical Security Procedures • Access Control Procedures

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

	• Use of Licensed Software Packages • Malicious code and Botnets and their prevention • Reporting and mitigation of incidents • Cyber Crisis Management • Implementation of Information Security Guidelines The security awareness, education, and training activities should be suitable and relevant to the person's role, responsibilities and skills. Training to enhance awareness is intended to allow individuals to recognize information security problems and incidents, and respond according to the needs of their work role and responsibility in event of violation of Standard Information Security guidelines.
Coordination and Incidents information sharing	All organisations should strive to improve coordination and communication with CERT-In, stakeholders, Ministry/department and other designated agencies and should share all information pertaining to cyber security incidents with CERT-In and other designated agencies. Cyber Security exercises conducted by CERT-In may be used as a tool for improving the coordination and information sharing.

4.2 Deployment of Information Security experts

Given the size of the problem and increasing threats of cyber terrorism, there is a need to deploy more experts in this field. A large number of security experts could be working on emerging vulnerabilities and effective defences. Periodic training may be provided to information security experts to update the skills with respect to latest technologies/threats and implementations.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

4.3 IT Security Best Practices Compliance-Levels of Assurance

In order to assist organisations in government as well as critical sectors to follow a roadmap for progressively achieving compliance and assurance w.r.t. IT security best practices, different levels of assurance have been conceived. Using these levels of assurance and the methods of verification, organisations can carry out self-assessment with regard to their present status of compliance assurance and declare the same accordingly. It is expected that these levels of assurance will also help the organisations in improving the maturity of their IT security management system as well as enhancing predictability and proactive nature of their system. Levels of Assurance are available at "**Appendix XI**"

<mention name of the organisation/Ministry/State Government/UT Government> is at level <1/2/3/3+/4/4+/4++> as on <year>. (Refer Appendix XI)

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

5 Cyber Crisis Recognition, Mitigation and Management

5.1 Incident Recognition

Recognition of cyber crisis depends on clearly identifying the cyber incidents. The crises arising out of cyber attacks are categorised and prioritised from level 1 to Level 4. The color in the table 5.1 below outlines the threat levels, spread of attack and related conditions that become the basis for declaration of a crisis. The table also outlines the crisis/contingency affecting the systems of individual organisation, multiple organisations, states and nation leading to crisis of different levels. The levels of crisis are interrelated. Each subsequent level will follow preceding one. No level other than level 1 will come in isolation.

Table 5.1 : Cyber security emergency – Levels of concern

Threat Level	Condition
Level 1 **Guarded** **Scope:** **Individual** **Organisation**	Perceptible change/variation in system performance and discovery of critical/non critical vulnerabilities/exploits and attacks that can affect normal operation of network and IT systems of individual organisation such as: • Targeted attacks and espionage activities. • Identity theft (Phishing, spoofing, social engineering etc.) • Web defacements and Application level attacks • Visible signs of malicious programs (viruses/worms/ Bots/malware/Keyloggers/Spyware/etc) • Detection of new and advanced malware infections • Attempts for exploitation of zero-day vulnerabilities • Denial of service attacks (DoS) • Distributed Denial of Service (DDoS) and Distributed Reflection Denial of Service (DrDoS) • Hacking of IT systems such as computers systems, Servers (Mail, Web, Database etc) and Routers • Spam

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Level 2 **Elevated** **Scope:** **Multiple Organisations**	Perceptible change/variation in network/ system performance and abnormal surge in network traffic affecting IT infrastructure of multiple organisations simultaneously due to: • Targeted attacks and espionage • Large scale infection of viruses/worms/ Bots/malware/ Keyloggers/Spyware for malicious and espionage activities • Detection of domain specific malwares like "stuxnet" targeting Industrial Control Systems • Focused attempts of network scanning and penetration • DDoS attacks and Distributed Reflection Denial of Service (DrDoS) • Attacks on Domain Name Servers, ,Mail Servers, Databases, Routers etc • Large scale web-application attacks like backdooring and defacement. • Attacks on Trust infrastructure • Attack on the IT infrastructure of a Critical Information System • Infection of computer systems and/or Programmable Logic Controller s (PLCs) • Abnormal functioning of SCADA/Industrial Control Systems
Level 3 **Heightened** **Scope:** **State/** **Multiple States**	Significant breakdown of supplies or services essential to the life of the citizens *including but not limited to* financial, Government, transport, energy or communication due to focused cyber-attacks on infrastructure of critical sector and Government across a state or multiple states.
Level 4 **Serious** **Scope:** **Entire Nation**	Significant/complete breakdown of supplies or services essential to the life of the citizens including but not limited to financial, Government, national defense, transport, energy or communication due to focused cyber-attacks on infrastructure of critical sector and Government across the nation.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

5.2 Cyber Crisis Management – Roles and Responsibilities

The following paragraphs outline the roles and responsibilities of various stakeholders of *<mention name of the organisation/Ministry/State Government/UT Government>* in dealing with cyber crisis. It is to be noted that cyber attacks on the IT infrastructure may simultaneously take place from different sources and on different targets including sensitive, military, civilian and critical infrastructure. Since a cyber incident may rapidly spread across interdependent and cross-jurisdictional networks and significant cyber incidents may quickly require nationally coordinated response actions based on differing authorities and priorities. The identification of expected roles will enable the affected organisation to expeditiously report the incident to the response teams in respective sectors. The latter may have to work together with other Incident Response Teams to mitigate the incident. Each organisation having specific roles and responsibilities during a cyber incident are also expected to routinely share information, collaborate and at times take part in joint actions involving other Central Administrative Ministries/Departments/Crisis management Group (CMG). The exact nature of support relationship will depend on the nature, severity and scope of each incident. *<Kindly refer IX for points of action for preparation of sectoral and organisational Cyber Crisis Management Plans >*

5.2.1 Crisis Management Group

(Applicable only for Central Ministries/Organisations)

The composition of the Crisis Management Group of <mention name of the organisation / Central Ministry> is indicated below:

In case of Central / State government Ministries

(a) Secretary	... Chairman
(e)	... Member
(l)	... Member Convener

In case of Organisations

(a) Head of the organisations	... Chairman

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

(e) ... Member

(l) ... Member Convener

The Crisis Management Group will be mainly responsible for dealing with the crisis situation in consultation with CERT-In and nodal ministry/department/organisation.

5.2.2 State Level Crisis Management Committee *(Applicable only for State Govts/UTs)*

The State Level Crisis Management Committee (SCMC), an apex body of high-level officials of the <State/UT> Government for dealing with a major crisis, which has serious or national ramifications, will also deal with State level crisis arising out of focused cyber-attacks. The composition of the Committee is as under:

(a) Chief Secretary ... Chairman

(b) Secretary/Principal Secretary ... Member

(c) ... Member

(d) ... Member

(e) ... Member

..

..

..

(l) ... Member Convener

The SCMC will be free to co-opt members depending on the nature of crisis, as and when required.

When a situation is handled by the SCMC it will give such directions to the Crisis Management Group of the Nodal Ministry/Department as deemed necessary.

5.2.3 Indian Computer Emergency Response Team (CERT-In)

CERT-In monitors Indian cyberspace and coordinates alerts and warning of imminent attacks and detection of malicious attacks among public and private cyber users and organisations in the country. It maintains 24x7 operations centre and has working relations/collaborations and contacts with CERTs all over the world; and

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Sectoral CERTs, public, private, academia, Internet Service Providers and vendors of Information Technology products in the country. It would work with Central Ministries and monitors cyber incidents on continuing basis throughout the extent of incident and would analyse and disseminate information and guidelines. The primary constituency of CERT-In would be all organisations other than Defence, Space, Atomic Energy, Law Enforcement and security agencies and their critical infrastructure.

5.2.4 National Critical Information Infrastructure Protection Centre (NCIIPC)

NCIIPC is a designated agency to protect the critical information infrastructure in the country. It gathers intelligence and keeps a watch on emerging and imminent cyber threats in strategic sectors including National Defence. It would prepare threat assessment reports and facilitate sharing of such information and analysis among members of the Intelligence, Defence and Law enforcement agencies with a view to protecting these agencies' ability to collect, analyze and disseminate intelligence. NCIIPC would interact with other incident response organisations including CERT-In, enabling such organisations to leverage the Intelligence agencies' analytical capabilities for providing advanced information of potential threats.

5.2.5 <Identify other key stakeholder>

<Identify other key stakeholder organisations involved in crisis management actions including their roles and responsibilities along with interface with other stakeholders>

5.2.6 <Identify the service providers>

<Identify the service providers involved in providing services like website, email, etc.>

5.2.7 Private Sector

Collaborative involvement of private sector is necessary to effectively protect the cyber domain and to counter the threats to cyber infrastructure. Since technological threats evolve quickly, the private sector can play an important role in innovating and mitigating threats, building security into applications & systems,

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

educating and raising awareness. The private sector would also be required to collaborate with their sectoral CERTs on threats, incidents, vulnerabilities, best practices and trend definition.

5.2.8 Control Room of the Ministry/State/UT

The respective Nodal Central Ministry / State Govt. / UT will setup a Control Room which would be activated immediately after a crisis situation is reported. A senior officer from the existing hierarchy of respective Nodal Central Ministry/State Govt. /UT should be designated as in-charge of Control Room who would draw up a plan for its manning during crisis situations on a 24-hour basis. Hot line facilities wherever necessary may be setup in consultation with the Department of Telecommunications. There would be a well laid out drill for the Control Room and the personnel expected to man it should be adequately trained in Control Room duties. Names, telephone numbers, cellular mobile phone numbers and addresses of Members and Alternate Members of Nodal Central Ministry/State Govt. / UT and various stake holders will be kept in the Control Room.

5.2.9 Reporting of Cyber Crisis

As and when a cyber crisis situation develops, respective organisations will immediately convey to the respective Nodal Central Ministry/State Govt/UT through any quickest possible means. Further, all organisations will take all necessary actions as given in Appendix III of this document and also report the incident to CERT-In in the manner and format as prescribed in Appendix XIII of this document.

5.2.10 Response System

Immediately on the occurrence of a cyber-crisis, the Contingency Plan would be put into effect by the respective organisations. The response action will be initiated in consultation with CERT-In, if the situation has wider ramifications and warrants response at the state/national level. The Nodal Central Ministry/State Govt/UT would activate its Control Room and summon a meeting of the Crisis Management Group to oversee the implementation of its Contingency Plan.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

5.2.11 Contact Information

Names, telephone numbers, cellular mobile phone numbers and addresses of Members and Alternate Members of various stakeholders are given in the Annexure I respectively.

5.3 Incident Response and Mitigation

General Guidelines on Cyber Crisis Management and security of Critical Infrastructure are outlined in Appendix VI. Table A12.1. Appendix XII outlines the nature of crisis/contingency affecting the systems of individual organisation, multiple organisations, states and nation leading to crisis of different levels and authorities responsible for mitigation along with agencies that support mitigation actions. The steps necessary to mitigate crisis will vary with respect to nature and severity of crisis. Respective authorities responsible for mitigation of a crisis will report the incident to the designated supporting organisations as mentioned in Chapter 5.2.

<Refer "Table A 12.1: Nature and Severity of cyber crisis, Authorities responsible and steps for mitigation" given in Appendix XII of *this document to derive and create a new set of table as applicable to your situation>*

5.4 Media Management

A media forms a vital link between those responding to crisis situation and the outside world. Besides this, media also can help in educating all concerns about crisis prevention and preparedness. It is recognized that unbiased and comprehensive media coverage can effectively aid the crisis response & resolution process and also enhance public confidence in the ability of organisations to respond to crisis. Accordingly, media management is a crucial issue in terms of pre-incidents as well as post incident information flow. In order to make best possible use of this vital link, it is necessary that media is given clear information and regular updates to enable them to perceive right picture and proportion of the crisis. In this context, it is also necessary for the organisations responding to cyber security incidents to identify responsible person of suitable level that has access to correct & updated information and is adequately trained for proper & consistent communication and avoid contradiction at all times.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

6 Post Incident Activity

After successful mitigation and recovery from incident, the following need to be undertaken (before closing the incident) for future reference/precaution:

- Perform a postmortem analysis of the incident as well as the incident response adopted at the organisation and CERT-In level
- Evaluate and perform assessment of the attack from the technical point of view in order to fine-tune and optimize the eradication mechanism
- Document lessons learnt from the incident and prepare incident report, including infrastructure protection improvements from the postmortem process
- Share incident report with CERT-In for future precaution and mitigation of similar attacks
- All critical organisations to implement infrastructure protection improvements resulting from postmortem reviews or other protection improvement mechanisms

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Appendix - I Planning and Preparation for Incident Handling (ISO 27035)

Proper and advanced planning ensures the response activities are known, coordinated and systematically carried out. It also facilitates the organisation and its functional department concerned to make appropriate and effective decision in tackling cyber security incident, and in turn minimizes the possible damages caused. The plan includes strengthening of cyber security protection, making appropriate response to the incident, recovery of the system and other follow up activities. Major activities involved in planning and preparation are as follows:

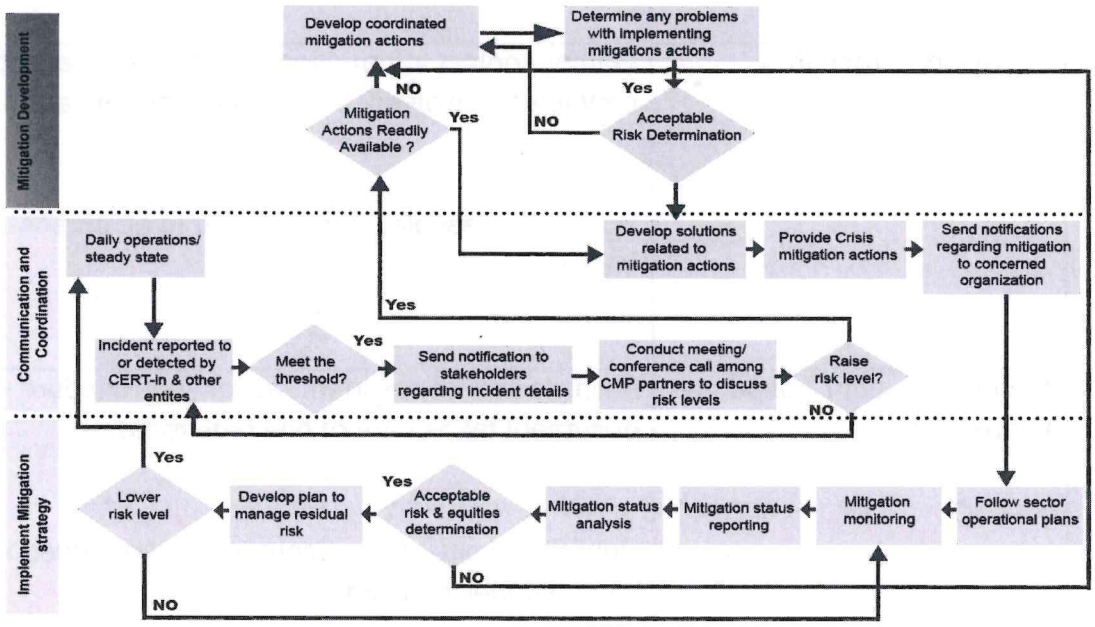
Sr. No.	Item	Details
1	Cyber Security Incident Handling Plan	Plan for Security Incident Handling – this document takes care of this requirement
2	Reporting Procedure	Design and prepare for the reporting mechanism(s) Publish the report mechanism(s) to all staff
3	Escalation Procedure	Gather contact information for all personnel to be contacted / involved, both internal and external. Publish the escalation procedure to all personnel involved.
4	Security Incident Response Procedure	Prepare security incident response procedure - This document takes care of this requirement. Publish the security incident response procedure to all personnel involved.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

5	Training and Education	Provide training to operation and support staff on knowledge in handling security incidents. This can be done as part of the induction process for any recruit in the functional group. Ensure staff are familiar with the incident response process.
6	Incident Monitoring Measure	Monitor and measure various parameters related to incidents and ensure that these are reviewed as part of regular functional group meetings.

The following flowchart depicts the broad incident management process and related actions:

Incident Management process



File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Appendix – II Incident Handling Team Structure

1.1 Notification Team

An incident can be reported by anyone; however it is typically reported by one of the following persons/ groups involved in managing and monitoring resources/ services:

- IT Infrastructure [particularly Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) / Router Monitoring Team]
- Network & System Support (NSS) Engineers
- Administration (Physical Security) Team
- Internal / External Audit Team
- Associates

Responsibility

An Associate / team discovering the incident is responsible for communicating the same to the Service Desk Team immediately. Incidents must be assigned the appropriate severity level by the associate / team at the time of reporting the incident.

1.2 The Service Desk Team

The Service Desk is the place in the organisation where all security incidents are to be registered by issuing a service ticket. Efficient and effective reaction to security incidents demands a formal method of working that can be supported by software tools.

Incidents that cannot be resolved immediately by the Service Desk are to be assigned to the concerned functional group for that location. A resolution or work-around should be established as quickly as possible in order to restore service to users with minimum disruption to their work. After resolution of the cause of the incident and restoration of service, the incident is closed.

Throughout an incident life cycle it is important that the service ticket is maintained. Even in cases where the incident is reported by a phone call / email, the

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

ticket must be raised by the service support team member. This allows any member of the support team to provide an up-to-date progress report.

1.3 Cyber Crisis Detection and Prevention

Cyber crisis detection and prevention is ensured 24 hours a day via the Administration, Human Resource and Information Security staff together with all involved project delivery staff. All these services would co-operate towards the prevention and handling of a cyber crisis. It is the concerned associate on duty who is responsible for alerting the Crisis Management Cell (CMC) of an imminent serious crisis.

1.4 Level I Incident Resolution Team

Each location of the organisation should have an identified list of personnel who will be part of the respective Level I Incident Resolution team.

Responsibilities

- Identify the correctness of the severity level
- Contain, Eradicate and Recover
- Seek necessary resources and support from the corresponding Level II Incident Resolution Team
- Provide regular updates to corresponding Level II Incident Resolution Team and the Crisis Management Cell (CMC) regarding progress of the incident handling process
- Escalate to the corresponding Level II Incident Resolution Team, if unable to resolve within the prescribed time frame/reasonable time frame.

1.5 Level II Incident Resolution Team

The team involves CISO, his team, Admin, HR functional groups. This team should have full authority to undertake any actions or decisions necessary to contain, eradicate and recover the situation.

Responsibilities

- Provide support to the Level I Incident Resolution Team to facilitate prompt containment, eradication and recovery of the affected entity

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

- Communicate to all responsible parties and stakeholders like Project Managers and Onsite Account Managers including customer's contact (if warranted in the agreement) and Crisis Management Cell (CMC) within the organisation.
- Maintain contact with CERT-In and the respective nodal agency.
- Supervise and coordinate all security incident handlings for the functional group at the particular location
- Facilitate experience and information sharing on security incident to CMC, CERT-In and respective nodal agency.

Appendix – III Incident Response activities during the First Hour

1.0 Introduction

The primary objective of incident response actions during first hour is to contain the damage due to the incident, notify appropriate authorities about the incident and ensure continuity of essential activities and services of the organisation.

The following guidelines describe the actions to be taken within the affected organisation during the first hour of incident. The guidelines also facilitate detailed incident analysis and determination of recovery and response actions and possible escalation within and outside the organisation.

2.0 Triggers for first reaction

The reaction by the users or administrators within an organisation could be triggered by observation of certain symptoms and anomalies in the functioning of systems, networks and processes. The trigger for response action could be infection, attack or intrusion or malfunctioning of a system. Further the actions could be triggered when alerts are received from external organisations such as CERT-In and other Incident Response teams and security agencies.

2.1 Means of Detection

The means of detecting anomalies and abnormal conditions that require response actions are Users, System/Network Administrators, technical tools and external alerts from security agencies such as CERT-In.

3.0 Symptoms of incidents and response actions

Table A 3.1 outlines the general symptoms indicating occurrence of incident noticeable by all types of users, source of detection, response actions required and persons responsible for the actions.

Table A 3.2 outlines Indications of different types of Cyber Crises generally noticeable by trained users, System Administrators & tool based detection

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

mechanisms and response actions required and authorities responsible for the actions

Table A 3.1 General symptoms of incidents noticeable by all types of users & System Administrators and related response actions

Symptoms/Alerts	Source of detection	Response actions	Who to handle
Common Symptoms			
Non-availability of computer system (failure to start)	User	Boot with alternate OS/ recovery media. Check the booting process for specific errors. Report to the System administrator	User System Administrator
Frequent system crashes Unexplained, poor system performance Presence of new files Presence of unknown processes Changes in the file size or dates	User	Scan system with updated Antivirus & Anti-spyware Report to the System administrator	User System Administrator
New suspicious user accounts	User	Report to the System administrator	System Administrator
Failed or successful social engineering attempts	User System Admini-strator	Collect all details such as email content, header etc and examine. Alert other users	System Administrator
Failed log in attempts by unauthorized users	Technical tools Supervisory review of logs	Determine the timing, sources of activities Trace the attack sources from logs of system/directory server.	System Administrator
Unusual time of usage Unauthorised user	Super-visory Review of logs	Correlate with physical access by users Correlate with logs of perimeter	System Administrator Network

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

accounts		devices to find external intrusion	Administrator
Symptoms/Alerts	**Source of detection**	**Response actions**	**Who to handle**
Virus/worm infection/lockdown of resources by unauthorized encryption	User System Administrator	Disconnect system from network Boot with different OS and scan with Antivirus & Anti-spyware Antivirus and Anti-spyware should be updated regularly	User System Administrator
Suspicious probes	Technical tools (IDS/IPS/ Firewall)	Close the ports and services which are not required Send the logs to Incident Response team for examination	Network Administrator
Abnormal surge in traffic (inbound/outbound)	Technical tools Network Behaviour Analysis Router	Trace the specific service/protocol Detect the source of generation of abnormal traffic Correlate with alerts from CERT-In	Network Administrator
External Alerts			
Alert for new vulnerability	CERT-In	Apply appropriate patches/updates Implement suggested workarounds for zero-day vulnerabilities	System Administrator
Alert on propagation of malicious code	CERT-In	Update the Antivirus signatures Follow the countermeasures suggested in the specific advisory and in this table	System Administrator
Alert indicating attack sources	CERT-In Security agencies	Block the attack sources notified by CERT-In and other agencies	Network Administrator

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Table A 3.2 Indications of different types of Cyber Crises generally noticeable by trained users, System Administrators & tool based detection mechanisms and Response actions.

Symptoms/Indications/Alerts	Source	Response actions	Who to handle
Website defacement and semantic attacks			
Detection of defacement/ intrusion of website	Users Website administrators External agencies	Disconnect the webserver hosting defaced/compromised website Examine the compromised system/website for specific unathorised changes Restore the website content, Shift and run website from a different trusted system by making appropriate DNS changes at the new system Collect relevant logs of server and application and submit to IR team of organisation Report the incident alongwith logs to CERT-In	Website Administrator Network Administrator
Malicious Code attacks (virus/worm/ /Trojans/Botnets/Spyware/ransomware)			
Unexplained poor system performance Presence of suspicious process/files on system Suspicious/un-authorised changes to system files, configuration files (eg. Hosts file) Unauthorized encryption of the systems/files. Surge in traffic on	Users System Administrator Alerts from Antivirus, NIDS External agencies	Disconnect infected systems from network Scan with updated Antivirus and Anti-spyware Recover from clean backup. Apply appropriate countermeasures in consultation with local Incident Response team/CERT-In	System Administrator

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

ports/services used by malware Connections to suspicious remote systems Unusual ports open			
SPAM attacks			
Abnormal surge in SMTP traffic Bandwidth congestion Slow response of mail servers	Users Network Admini-strators Network Behaviour Analysis	Check the mail servers for open relays and disable Close ports not required in the Mail server Identify possible sources of Spam from email headers and invoke blacklists such as SBL, XBL and PBL If attack persists report to local Incident Response Team/CERT-In	Network Administrator Mail server Administrator
Attack on ICS and IoT/IIoT devices			
Backdoor detection. Abnormal functions. Data exfiltration. Alerts in Monitoring & detection systems	Service Consumers OT Team IT Team External Agencies	Check for signs of infection or compromise in IoT/IIoT devices or ICS environment including HMI & Business network. Identify vulnerability exploited. Isolate infected devices from all networks immediately Report the incident to local IR Team/CERT-In at the earliest. Consult relevant advisories of CERT-In and follow specific measures suggested therein Take a forensic image and send to local IR Team/CERT-In update the affected systems with the relevant patch/workaround.	IT and OT Team

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Supply Chain Attacks			
Backdoor detection. Malicious functions/operations of devices. Malicious traffic originating from network. Detection of data exfiltration.	Network Administrator SOC team Vendor/Supplier External Agencies	Isolation of affected systems/products from Network. Coordinated vulnerability Mitigation. Identification of workaround. Impact analysis. Review of SLAs, Policies and controls. Reporting of Incidents to relevant agencies.	Network Administrator SOC team Vendor/Supplier
Attacks on Mail Servers			
Non availability mail accounts Compromised mail accounts	Users Mail server administrator	Mail server compromise: Disconnect mail server Activate standby mail server Check logs of mail server and identify attack source Send the logs to Incident Response Team/CERT-In User account compromise: Reset the password Enforce strong passwords (minimum 8 digit and alphanumeric) Enforce email best practices	Mail server Administrator
Identity Theft Attacks through spoofing			

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

300

Detection of suspicious network connections Detection of Packets with suspicious source address Emails from masqueraded account name	Alerts from IPS/IDS Email headers	Examine the email header and find the actual origin of email Notify and alert users To counter spoofing, implement Egress and Ingress filtering at perimeter (Router) Enforce email authentication Report to local Incident Response Team/CERT-In	Network Administrator
Phishing attacks			
Reporting of phishing email/website	Users Anti-phishing/ fraud detection services CERT-In/ external agencies	Report phishing incident to local IR Team/CERT-In Report phishing URL to phishing filters Send phishing emails and details of phishing website to CERT-In	Users Designated persons
Denial of Service (DoS) attacks			
Non availability of services such as website, email etc System crashes Bandwidth congestion Surge in traffic	Users Website Admini-strator	Identify the type of attack such as flooding of particular types of packets/requests (TCP SYN, ICMP etc) by examining logs of Router / IPS / IDS / Firewall Identify the attack sources Block the attack sources at Router/Packet filtering device Check Router configuration and implement Egress and Ingress filtering to block spoofed packets Disable the non essential ports/services Report to local Incident Response Team/CERT-In with relevant logs	
Distributed Denial of Service (DDoS) attacks			
Non availability of	Network	Identify the type of attack such as	Network

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

services such as website, email etc System crashes Bandwidth congestion Surge in traffic	Administrator Alerts of IPS/IDS/ Firewalls Network Behaviour Analysis CERT-In	flooding of particular types of packets/requests by examining logs of Router/IPS/IDS/ Firewall Apply appropriate rate limiting strategies at the local perimeter and if necessary consult ISP Implement Egress and Ingress filtering to block spoofed packets Use appropriate DoS prevention tools If problem persists shift web/mail services hosting to alternate Internet Protocol addresses (IPs) Report to local Incident Response Team/CERT-In with relevant logs	Administrator
DoS Attacks on DNS server			
Slow response or non-availability web/mail services	User Network Administrator	Change the Primary DNS Server Implement Source address validation through ingress filtering (Implement IETF BCP 38/RFC 2827) Use Unicast Reverse Path Forwarding to mitigate problems that are caused by malformed or forged IP source addresses Run separate DELEGATED and RESOLVING name servers Disable Recursion on DNS server authoritative for the zone Restrict zone transfers to Secondary name servers only Block invalid DNS messages to an authoritative name server at the network edge. This includes blocking large IP packets directed to an authoritative name server. Report to local Incident Response Team/CERT-In	Network Administrator

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

302

DNS Cache poisoning attacks			
Redirection of legitimate web/mail traffic to suspicious websites/mail servers	User Network Administrator	Purge cache Restart DNS server Replace DNS records with content from trusted backup Examine DNS forwarding traffic to identify rogue DNS server and block Restrict rights of configuration changes to Administrator only At client side, delete any additional entries in HOSTS file Report to local Incident Response Team/CERT-In	Network Administrator
Application Level attacks			
Unauthorised changes to Data Suspicious user activity Elevation of privilege of user accounts Presence of malicious links/content	Web/ Database Administrator Application logs	Disable suspected user accounts Reduce the interactive features and run with minimum essential features Restore data from trusted backup Identify attack sources from application logs and block Enforce Input validation Apply latest patches/updates Report to local Incident Response Team/CERT-In	Web Administrator Database Administrator
Router level attacks			
Unexplained packet loss Non availability of gateway/ Internet services	Users Network administrator Review of Router configurations	Replace the router with a securely configured standby router with Egress and Ingress filtering Check the logs and configuration files of compromised router to identify attacks Replace the configuration files with trusted backup Apply appropriate patches/updates Block the attack source Report to local Incident	Network Administrator

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

		Response Team/ Service Provider/CERT-In	
High Energy RF based Denial of Services Attacks			
Non availability of wireless connectivity Degraded Signal to Noise Ratio Increased Noise levels in the airwaves	Users Network Administrator Alerts of IDS/IPS	Identify the other devices due to which RF interference occurs and physically remove them. Detect rouge access points and remove them If attack persists switch critical functions to wired networks Report to local Incident Response Team/CERT-In	Network Administrator
Targeted Scanning, Probing and Reconnaissance of Networks and IT Infrastructure			
Huge amount of IPS/IDS alerts High volume of dropped packets by Firewalls Surge in specific traffic	User Network Admini-strator Logs of relevant devices	Identify the type of scans/probes by examining logs of Router/IDS/ IPS/Firewall Identify the sources of scans Block the sources of scanning Report the incidents with relevant logs to CERT-In/other incident response teams	Network Administrator

4.0 Conditions for escalation and detailed analysis

It is quite possible to come to a conclusion that there would be situations that call for:

- Actions within the organisation
- Actions beyond an organisation

The users observing the symptoms/indications mentioned in Table A 3.1 and A 3.2 should immediately report the same to concerned system/network administrator or designated authority within the organisation.

The System/Network administrators should escalate the reports of incidents affecting or could affect critical business functions or services to appropriate authorities within the organisation, local Incident Response Team and CERT-In.

After the response actions within 1st hour of incident, the procedures and actions described in the **Appendix III** "Incident response during first 24 hours" need to be followed for detailed incident analysis and follow-up actions.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

304

5.0 What needs to be reported to CERT-In

The following cyber security incidents must be reported to CERT-In in the format prescribed in **Appendix XIII**, within one hour of occurrence of the incident or noticing the incident.

- Targeted scanning/probing of critical networks/systems
- Compromise of critical systems/information
- Unauthorised access of IT systems/data
- Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.
- Malicious code attacks such as spreading of virus/worm/Trojan/Botnets/Spyware
- Attacks on servers such as Database, Mail and DNS and network devices such as Routers
- Identity Theft, spoofing and phishing attacks
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Attacks on Critical infrastructure, SCADA Systems and Wireless networks
- Attacks on Applications such as E-Governance, E-Commerce etc.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Appendix – IV Information Security Management System (ISMS)

Information Security and Management

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organisational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organisation are met.

An Information Security Management System (ISMS) is a systematic approach to managing sensitive information of an organisation so that it remains secure. The adoption of an information security management system is a strategic decision for an organisation. It encompasses people, processes and IT systems.

Information Security Standards

International Organisation for Standards (ISO) has published the following standards to enable organisations to establish and implement ISMS effectively:

ISO 27001 - Information Security Management Systems – Requirements

ISO 27002 - Code of Practice for Information Security Management

These standards codify industry experience and security best practices, and are applicable to all types of organisations, irrespective of their size or business.

ISO 27002 is a guidance standard and provides detailed advice on the nature and implementation of security controls for an effective ISMS. This standard covers guidance on managerial, technical and operational aspects of security controls of ISMS.

ISO 27001 is a standard that allows organisations to benchmark their ISMS and check its compliance status through an independent third party audit leading to certification. The process approach for information security management presented in this International Standard encourages its users to emphasize the importance of:

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

1. A committed top management having top down strategy with well-defined authority and accountability for the practices of ISMS.

2. A well-defined policies and procedures which are in line to the business objective of the organisation. Some key focus areas as also emphasized by ISO/IEC 27001:2013 :-

    a. What is to be done?
    b. How is to be done?
    c. What recourses would be required?
    d. Who will be responsible?
    e. When it gets completed?
    f. How to evaluate result?
    g. Measurable result?

3. Implementing and operating controls to manage an organisation's information security risks in the context of the organisation's overall business risks;

4. Monitoring and reviewing the performance and effectiveness of the ISMS

5. Continual improvement and evaluation based on objective measurement

This Standard provides a robust model for implementing the principles governing risk assessment, security design and implementation, security management, reassessment and continual improvement. The requirements set out in ISO 27001 are generic and are intended to be applicable to all organisations, regardless of type, size or nature.

Implementing an ISMS

The following steps will help an organisation in implementing ISMS:

Step-1: Undertaking comprehensive Security Audit to discover the gaps with respect to security best practices as per ISO 27001 standard. CERT-In has created a panel of IT Security auditors that can provide IT security-auditing services on commercial basis. The list of auditors is available on CERT-In website www.cert-in.org.in .

Step-2: Implementing corrective actions to close all gaps. This process can be undertaken internally or with the help of the CERT-In's panel of IT Security Auditors to derive necessary hand holding support to implement the corrective

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

307

actions. While doing so, use of same agency that was involved in Step-1 to be avoided, in view of potential conflict of interest.

Step-3: Obtaining independent third party endorsement. For this purpose, the services of an independent accredited third party ISMS certification agency may be taken.

ISMS Focus Areas

An effective ISMS includes:

- **Risk Assessment and Management (ISO 27005) -** Conducting periodic IT security risk assessments and determination of acceptable level of risks, consistent with criticality of business/functional requirements, likely impact on business/functions and achievement of organisational goals/objectives.
- **Policies and Procedures** – Preparing security policies and procedures in line with the international standard ISO 27001, addressing all aspects of managerial, technical and operational security controls. The following are some examples of security controls:
    - Conduct periodic back-up of files critical to mission accomplishment.
    - Storage of backup files should be isolated from any network and physically separated from the originating facility
    - Ensure procedures are in place that assures the appropriate physical and technical protection of the backup and restoration hardware, firmware and software, such as router tables, compilers and other security-related system software are done in a secure and verifiable manner.
    - Ensure remote access for privileged functions (i.e., access to system control, monitoring or administrative) is permitted only for compelling operational needs and establish strict controls.
    - Ensure remote access to user functions is mediated through a managed access control point (e.g., remote access server in DMZ).
    - Ensure Internet access for networks handling public information is permitted from a secured DMZ (Demilitarized Zone)

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

- **Security Plans** – Establishing detailed plans for securing networks, facilities, information systems, or groups of information systems, as appropriate (For ex. Patch management, virus protection etc.).
- **Managing Human Resource** - Human resource security ensures that the organisation's data handled by employees must be protected from unauthorized access, disclosure, interference, modification or destruction. Human resource security is necessary during all phases i.e. pre-employment, during employment and at the time of termination. Informing personnel through awareness trainings, about the information security risks associated with their activities and their responsibilities in complying with organisational policies and procedures that are designed to reduce these risks.

- **Safeguarding the Information Assets** - Asset management talks about the importance of identifying, tracking, classifying, and assigning ownership for the assets that holds the organisation's information in order to protect it adequately and fix accountability in case of loss or damage.

- **Protecting Access to critical information -** The allocation of access rights to users should be strictly controlled through user registration and administration procedures, including special restrictions over the allocation of privileges and passwords, and regular access rights reviews. All Information systems and applications should incorporate security controls to restrict unauthorized access.

- **Physically securing the Work areas/ Premises** - Physical security refers to measures taken to protect the system, premises and all supporting infrastructure against threats associated with physical and environmental security. Safeguards for Physical security are very important in protecting information to avoid damage or unauthorized access to information and systems.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

- **Securing Communications and Operations** - All communication and operation mediums must be properly safeguarded in order to ensure the secure exchange of data and information. It requires an effective network infrastructure management as well as well-defined procedures controls and responsibilities. The mechanism should be in place to protect the data at transit or at rest from unauthorized access by simply making it unreadable or unintelligible for the unauthorized users through techniques like cryptography.

- **Addressing Security during Information System Acquisition, Development & Maintenance** - Information Security must be addressed or taken into account at the time of acquiring, development and maintenance of the systems, software or application and for this a comprehensive quality assurance and control processes must be in place. Testing should also be done to determine whether the product meets the required security specifications prior to purchasing the product or moving the application to production.

- **Third Party Management** - Appropriate Controls and mitigation processes must be established with all suppliers in order to protect the shared information. In addition to protecting information handled and used by suppliers the organisation must regularly monitor and continuously assess the service level agreements and compliance.

- **Periodic Testing and Evaluation** —Periodically testing and evaluating the adequacy and effectiveness of technical security control measures implemented for IT systems and networks on an annual basis and after each significant change to the IT applications/systems/networks. This can include Penetration Testing, Vulnerability Assessment, Application Security Testing and Web Security Testing;

- **Independent Security Audits** – Engaging an independent IT Security auditing organisation to carry out Audit of ISMS on an annual basis.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

- **Incident Management (ISO 27035)** – Establishing procedures for detecting, and responding to security incidents and reporting to CERT-In.

- **Business Continuity and Disaster Recovery** – Developing and continuously updating plans and procedures to ensure continuity of critical operations and recovery within a reasonable time frame.

- **Compliance** – The governance of organisational security policies and procedures must comply with the best practices and standards and to minimize the risk and other negative consequences, the best practices, mandates of law, regulation and contractual requirement should be ensured.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Appendix – V Important Security Controls for Effective Cyber Security and Continuous Security Policy Compliance

"Establishing a prioritized baseline of information security measures and controls that can be continuously monitored through automated mechanisms."

Securing our Nation against cyber-attacks has become one of the highest priorities. To achieve this objective, networks, systems, and the operations teams that support them must vigorously defend against external attacks. Furthermore, for those external attacks that are successful, defenses must be capable of thwarting, detecting, and responding to follow-on attacks on internal networks as attackers spread inside a compromised network.

Security Controls for Effective Cyber Security and Continuous Security Policy Compliance

- Inventory and Control of Hardware Assets
- Inventory and Control of Software Assets
- Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- Continuous Vulnerability Management
- Controlled Use of Administrative Privileges
- Maintenance, Monitoring and Analysis of Audit Logs
- Email and Web Browser Protections
- Malware Defences
- Limitation and Control of Network Ports, Protocols, and Services
- Data Recovery Capabilities
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Boundary Defence
- Data Protection
- Controlled Access Based on the Need to Know
- Wireless Access Control
- Account Monitoring and Control

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

312

- Implement a security Awareness and Training Program
- Application Software Security
- Incident Response and Management
- Penetration Tests and Red Team Exercises

In general, organisations should examine all twenty control areas against their current status and develop an organisation-specific plan to implement the controls. Organisations with limited information security programs may choose to address certain aspects of the controls in order to make rapid progress and to build momentum within their information security program.

Insider Threats vs. Outsider Threats

A quick review of the critical controls may lead some readers to think that they are heavily focused on outsider threats and may, therefore, not fully deal with insider attacks. In reality, the insider threat is well covered in these controls in two ways. First, specific controls such as network segmentation, control of administrative rights, enforcement of need to know, data leakage protection, and effective incident response all directly address the key ways that insider threats can be mitigated. Second, the insider and outsider threats are merging as outsiders are more and more easily penetrating the security perimeters and becoming "insiders." All of the controls that limit unauthorized access within the organisation work effectively to mitigate both insider and outsider threats. It is important to note that these controls are meant to deal with multiple kinds of computer attackers, including but not limited to malicious internal employees and contractors, independent individual external actors, organized crime groups, terrorists, and nation state actors, as well as mixes of these different threats.

Furthermore, these controls are not limited to blocking only the initial compromise of systems, but also address detecting already-compromised machines, and preventing or disrupting attacker's actions. The defenses identified through these controls deal with decreasing the initial attack surface through improving architectures and hardening security, identifying already-compromised machines to address long-term threats inside an organisation's network, controlling so-called 'superuser' privileges on systems, and disrupting attackers' command-and-control of

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

implanted malicious code. Figure 1 illustrates the scope of different kinds of attacker activities that these controls are designed to help thwart.

The rings represent the actions computer attackers may take against target machines. These actions include initially compromising a machine to establish a foothold by exploiting one or more vulnerabilities (i.e., "Getting in"). Attackers can then maintain long-term access on a system, often by creating accounts, subverting existing accounts, or altering the software on the machine to include backdoors and rootkits (i.e., "Staying In"). Attackers with access to machines can also cause damage, which could include stealing, altering, or destroying information; impairing the system's functionality to jeopardize its business effectiveness or mission; or using it as a jump-off point for compromise of other systems in the environment (i.e. "Acting"). Where these rings overlap, attackers have even more ability to compromise sensitive information or cause damage. Outside of each set of rings in the figure, various defensive strategies are presented, which are covered throughout the controls described in this document. Defenses in any of the rings helps to limit the abilities of attackers, but improved defenses are required across all three rings and their intersections. It is important to note that the guidelines are designed to help improve defenses across each of these rings, rather than on merely preventing initial compromise.

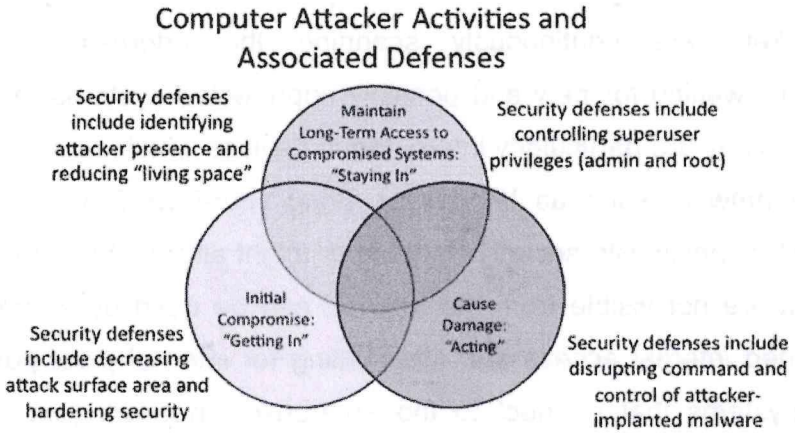


Figure 1: Computer Attacker Activities and Associated Defenses

Periodic and Continual Testing of Controls

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Each control included in this document describes a series of tests that organisations can conduct on a periodic or, in some cases, continual basis to ensure that appropriate defenses are in place. One of the goals of the tests described in this document is to provide as much automation of testing as possible. By leveraging standardization efforts these automated test suites and scripts can be highly sharable between organisations, consistent to a large extent, and easily used by auditors for validation. However, at various phases of the tests, human testers are needed to set up tests or evaluate results in a fashion that cannot be automated. The testers associated with measuring such controls must be trusted individuals, as the test may require them to access sensitive systems or data in the course of their tests. Without appropriate authorization, background checks, and possibly clearance, such tests may be impossible. Such tests should also be supervised or reviewed by appropriate agency officials well versed in the parameters of lawful monitoring and analysis of information technology systems.

DESCRIPTION OF CONTROLS

Control 1: Inventory and Control of Hardware Assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Attackers are continuously scanning the address space of target organisations, waiting for new and possibly unprotected systems to be attached to the network. They are particularly interested in devices which come and go off of the enterprise's network such as laptops or Bring-Your-Own-Devices (BYOD) which might be out of synch with security updates or might already be compromised. Even devices that are not visible from the Internet can be used by attackers who have already gained internal access and are hunting for internal pivot points or victims. Additional systems that connect to the enterprise's network (e.g., demonstration systems, temporary test systems, guest networks) should also be managed carefully and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

This Control requires both technical and procedural actions, united in a process that accounts for and manages the inventory of hardware and all associated information throughout its life cycle. It links to business governance by establishing information/asset owners who are responsible for each component of a business process that includes information, software, and hardware. Organisations can use large-scale, comprehensive enterprise products to maintain IT asset inventories. Others use more modest tools to gather the data by sweeping the network, and manage the results separately in a database.

Critical Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Attackers continuously scan target organisations looking for vulnerable versions of software that can be remotely exploited. Some attackers also distribute hostile web pages, document files, media files, and other content via their own web pages or otherwise trustworthy third-party sites. When unsuspecting victims access this content with a vulnerable browser or other client-side program, attackers compromise their machines, often installing backdoor programs and bots that give the attacker long-term control of the system.

Managed control of all software also plays a critical role in planning and executing system backup, incident response, and recovery.

Whitelisting can be implemented using a combination of commercial whitelisting tools, policies or application execution tools that come with anti-virus suites and popular operating systems. The best of these tools provide an inventory check of hundreds of common applications used in enterprises, pulling information about the patch level of each installed program to ensure that it is the latest version and leveraging standardized application names, such as those found in the common platform enumeration specification.

Critical Control 3: Continuous Vulnerability Management

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

An effective vulnerability assessment and remediation program must be able to prevent the exploitation of vulnerabilities by detecting and remediating vulnerabilities in covered devices in a timely fashion. Proactively managing vulnerabilities on covered devices will reduce or eliminate the potential for exploitation and save on the resources otherwise needed to respond to incidents after exploitation has occurred. Organisation units should define roles and responsibilities associated with vulnerability detection and remediation. Security roles defined in Security Contact application should be used to assign responsibilities for detecting and remediating against identified vulnerabilities.

Critical Control 4: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise. Two very common attacker techniques take advantage of uncontrolled administrative privileges. In the first, a workstation user running as a privileged user is fooled into opening a malicious email attachment, downloading and opening a file from a malicious website, or simply surfing to a website hosting attacker content that can automatically exploit browsers. The file or exploit contains executable code that runs on the victim's machine either automatically or by tricking the user into executing the attacker's content.

The second common technique used by attackers is elevation of privileges by guessing or cracking a password for an administrative user to gain access to a target machine. If administrative privileges are loosely and widely distributed, or identical to passwords used on less critical systems, the attacker has a much easier time gaining full control of systems, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges.

Critical Control 5: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers

Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Prevent attackers from exploiting services and settings that allow easy access through networks and browsers: Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.

All remote administration of servers, workstation, network devices, and similar equipment should be done over secure channels. Protocols such as telnet, virtual network computing (VNC), remote desktop protocol (RDP), or other protocols that do not natively support strong encryption should only be used if they are performed over a secondary encryption channel, such as secure sockets layer (SSL) or Internet protocol security (IPSEC).

Strict configuration management should be followed, building a secure image that is used to build all new systems that are deployed.

Critical Control 6: Maintenance, Monitoring and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Most free and commercial operating systems, network services, and firewall technologies offer logging capabilities. Such logging should be activated, with logs sent to centralized logging servers. Firewalls, proxies, and remote access systems (VPN, dial-up, etc.) should all be configured for verbose logging, storing all the information available for logging in the event a follow-up investigation is required. Furthermore, operating systems, especially those of servers, should be configured to create access control logs when a user attempts to access resources without the appropriate privileges. To evaluate whether such logging is in place, an organisation should periodically scan through its logs and compare them with the asset inventory in order to ensure that each managed item actively connected to the network is periodically generating logs.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Analytical programs such as SIEM solutions for reviewing logs can provide value, but the capabilities employed to analyze audit logs are quite extensive, even including, importantly, just a cursory examination by a person. Actual correlation tools can make audit logs far more useful for subsequent manual inspection. Such tools can be quite helpful in identifying subtle attacks. However, these tools are neither a panacea nor a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition are often required to identify and understand attacks.

Critical Control 7: Email and Web Browser Protections

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

Web browsers and email clients are very common points of entry and attack because of their technical complexity, flexibility, and their direct interaction with users and with the other systems and websites. Content can be crafted to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks. Since these applications are the main means for users to interact with untrusted environments, these are potential targets for both code exploitation and social engineering.

Critical Control 8: Malware Defenses

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

Malware defenses must be able to operate in this dynamic environment through large-scale automation, rapid updating, and integration with processes like incident response. They must also be deployed at multiple possible points of attack to detect, stop the movement of, or control the execution of malicious software. Enterprise endpoint security suites provide administrative features to verify that all defenses are active and current on every managed system.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

319

To ensure anti-virus signatures are up-to-date, organisations use automation. They use the built-in administrative features of enterprise endpoint security suites to verify that anti-virus, antispyware, and host-based IDS features are active on every managed system. They run automated assessments daily and review the results to find and mitigate systems that have deactivated such protections, as well as systems that do not have the latest malware definitions.

Critical Control 9: Limitation and Control of Network Ports, Protocols, and Services

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services, and Domain Name System (DNS) servers installed by default on a variety of different device types, often without a business need for the given service.

Port scanning tools are used to determine which services are listening on the network for a range of target systems. In addition to determining which ports are open, effective port scanners can be configured to identify the version of the protocol and service listening on each discovered port. This list of services and their versions are compared against an inventory of services required by the organisation for each server and workstation in an asset management system. Recently added features in these port scanners are being used to determine the changes in services offered by scanned machines on the network since the previous scan, helping security personnel identify differences over time.

Critical Control 10: Data Recovery Capabilities

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organisational effectiveness with polluted information. When the attackers are discovered, it can be extremely difficult for organisations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine.

Critical Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Attackers take advantage of network devices becoming less securely configured over time as users demand exceptions for specific business needs. Sometimes the exceptions are deployed and then left undone when they are no longer applicable to the business needs. In some cases, the security risk of the exception is neither properly analyzed nor measured against the associated business need and can change over time. Attackers search for vulnerable default settings, gaps or inconsistencies in firewall rule sets, routers, and switches and use those holes to penetrate defenses. They exploit flaws in these devices to gain access to networks, redirect traffic on a network, and intercept information while in transmission. Through such actions, the attacker gains access to sensitive data, alters important information, or even uses a compromised machine to pose as another trusted system on the network.

Critical Control 12: Boundary Defense

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Attackers focus on exploiting systems that they can reach across the internet, including not only DMZ systems but also workstations and laptop computers that pull content from the Internet through network boundaries.

To control the flow of traffic through network borders and police content by looking for attacks and evidence of compromised machines, boundary defenses should be multi-layered, relying on firewalls, proxies, DMZ perimeter networks, and network-based IPS and IDS. It is also critical to filter both inbound and outbound traffic.

It should be noted that boundary lines between internal and external networks are diminishing as a result of increased interconnectivity within and between organisations as well as the rapid rise in deployment of wireless technologies. These blurring lines sometimes allow attackers to gain access inside networks while bypassing boundary systems. However, even with this blurring of boundaries, effective security deployments still rely on carefully configured boundary defenses that separate networks with different threat levels, sets of users, data and levels of control. And despite the blurring of internal and external networks, effective multi-layered defenses of perimeter networks help lower the number of successful attacks, allowing security personnel to focus on attackers who have devised methods to bypass boundary restrictions.

Critical Control 13: Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

It is important that an organisation understand what its sensitive information is, where it resides, and who needs access to it. To derive sensitivity levels, organisations need to put together a list of the key types of data and the overall importance to the organisation. This analysis would be used to create an overall data classification scheme for the organisation. Organisations should define labels, such as "Sensitive," "Business Confidential," and "Public," and classify their data according to those labels. Once the private information has been identified, it can then be further subdivided based on the impact it would have to the organisation if it were compromised.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Once the sensitivity of the data has been identified, create a data inventory or mapping that identifies business applications and the servers that house those applications. The network then needs to be segmented so that systems of the same sensitivity level are on the same network and segmented from systems with different trust levels. If possible, firewalls need to control access to each segment.

Critical Control 14: Controlled Access Based on the Need to Know

The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Commercial tools are available to support enterprise management of encryption and key management within an enterprise and include the ability to support implementation of encryption controls within cloud and mobile environments.

Definition of life cycle processes and roles and responsibilities associated with key management should be undertaken by each organisation.

Commercial Data loss prevention (DLP) solutions are available to look for exfiltration attempts and detect other suspicious activities associated with a protected network holding sensitive information. Organisations deploying such tools should carefully inspect their logs and follow up on any discovered attempts, even those that are successfully blocked, to transmit sensitive information out of the organisation without authorization.

Critical Control 15: Wireless Access Control

Effective organisations run commercial wireless scanning, detection, and discovery tools as well as commercial wireless intrusion detection systems.

Major thefts of data have been initiated by attackers who have gained wireless access to organisations from outside the physical building, bypassing organisations' security perimeters by connecting wirelessly to access points inside the organisation.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Effective organisations run commercial wireless scanning, detection, and discovery tools as well as commercial wireless intrusion detection systems.

Additionally, the security team should periodically capture wireless traffic from within the borders of a facility and use free and commercial analysis tools to determine whether the wireless traffic was transmitted using weaker protocols or encryption than the organisation mandates. When devices relying on weak wireless security settings are identified, they should be found within the organisation's asset inventory and either reconfigured more securely or denied access to the organisation network.

Additionally, the security team should employ remote management tools on the wired network to pull information about the wireless capabilities and devices connected to managed systems.

Critical Control 16: Account Monitoring and Control

Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

Although most operating systems include capabilities for logging information about account usage, these features are sometimes disabled by default. Even when such features are present and active, they often do not provide fine-grained detail about access to the system by default. Security personnel can configure systems to record more detailed information about account access, and use home-grown scripts or third-party log analysis tools to analyze this information and profile user access of various systems.

Accounts must also be tracked very closely. Any account that is dormant must be disabled and eventually removed from the system. All active accounts must be traced back to authorized users of the system, and they should utilize multi-factor authentication. Users must also be logged out of the system after a period of inactivity to minimize the possibility of an attacker using their system to extract information from the organisation.

Critical Control 17: Implement a Security Awareness and Training Program

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

For all functional roles in the organisation (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organisational planning, training, and awareness programs.

An effective enterprise-wide training program should take a holistic approach and consider policy and technology at the same time as the training of people. Policies should be designed with technical measurement and enforcement and they should be reinforced by training to fill gaps in understanding; technical controls can be implemented to protect systems and data and minimize the opportunity for people to make mistakes. With technical controls in place, training can be focused concepts and skills that cannot be managed technically.

Critical Control 18: Application Software Security

Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

Attacks often take advantage of vulnerabilities found in web-based and other application software. Vulnerabilities can be present for many reasons, including coding mistakes, logic errors, incomplete requirements, and failure to test for unusual or unexpected conditions. Examples of specific errors include: the failure to check the size of user input; failure to filter out unneeded but potentially malicious character sequences from input streams; failure to initialize and clear variables; and poor memory management allowing flaws in one part of the software to affect unrelated (and more security critical) portions.

Critical Control 19: Incident Response and Management

Protect the organisation's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

After defining detailed incident response procedures, the incident response team should engage in periodic scenario-based training, working through a series of

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

attack scenarios fine-tuned to the threats and vulnerabilities the organisation faces. These scenarios help ensure that team members understand their role on the incident response team and also help prepare them to handle incidents. It is inevitable that exercise and training scenarios will identify gaps in plans and processes, and unexpected dependencies.

Critical Control 20: Penetration Tests and Red Team Exercises

Test the overall strength of an organisation's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

A successful defensive posture requires a comprehensive program of effective policies and governance, strong technical defenses, and appropriate action by people. Penetration testing starts with the identification and assessment of vulnerabilities that can be identified in the enterprise. Red Team exercises take a comprehensive approach at the full spectrum of organisation policies, processes, and defences in order to improve organisational readiness, improve training for defensive practitioners, and inspect current performance levels. Independent Red Teams can provide valuable and objective insights about the existence of vulnerabilities and the efficacy of defenses and mitigating controls already in place and even of those planned for future

implementation.

Penetration tests and Red Team tests are performed:

- as a "dramatic" demonstration of an attack, usually to convince decision makers of their enterprise's vulnerability;
- as a means to test the correct operation of enterprise defences ("verification"); and
- to test that the enterprise has built the right defences in the first place ("validation").

References

[1] CIS Critical Controls

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Appendix – VI Guidelines on Cyber Crisis Management and Security of Critical Infrastructure

1.0 Introduction

Critical networks contain computers and applications that perform key functions in providing essential services and commodities. As such, they are part of the nation's critical infrastructure and require protection from a variety of threats that exist in cyber space today. By allowing remote collection and analysis of data and control of equipment, critical networks provide great efficiency and are widely used. However, this makes critical networks potentially vulnerable to disruption of service, process redirection, or manipulation of operational data that could result in public safety concerns and/or serious disruptions to the nation's critical infrastructure.

2.0 Guidelines to improve security of critical networks

The guidelines prescribed in the following sections are intended to ensure that interruptions or manipulations of critical functions/services in critical sector organisations are brief, infrequent, manageable and cause least possible damage.

The following steps focus on specific actions to be taken to improve the security of critical networks:

2.1 Identify all connections to critical networks.

Conduct a thorough risk analysis to assess the risk and necessity of each connection to the critical network. Develop a comprehensive understanding of all connections to the critical network, and how well these connections are protected. Identify and evaluate the following types of connections:

- Internal local area and wide area networks, including business networks
- The Internet
- Wireless network devices, including satellite uplinks
- Modem or dial-up connections
- Connections to business partners, vendors or regulatory agencies

2.2 Disconnect unnecessary connections to the critical network.

To ensure the highest degree of security of critical systems, isolate the critical network from other network connections to as great a degree as possible. Any

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

connection to another network introduces security risks, particularly if the connection creates a pathway from or to the Internet. Although direct connections with other networks may allow important information to be passed efficiently and conveniently, insecure connections are simply not worth the risk; isolation of the critical network must be a primary goal to provide needed protection. Consider 'Air-Gap' for sensitive networks, following a risk assessment.

Strategies such as utilization of "demilitarized zones" (DMZs) and data warehousing can facilitate the secure transfer of data from the critical network to business networks. However, they must be designed and implemented properly to avoid introduction of additional risk through improper configuration.

2.3 Evaluate and strengthen the security of any remaining connections to the critical network.

Conduct penetration testing or vulnerability analysis of any remaining connections to the critical network to evaluate the protection posture associated with these pathways. Use this information in conjunction with risk management processes to develop a robust protection strategy for any pathways to the critical network. Since the critical network is only as secure as its weakest connecting point, it is essential to deploy firewalls, intrusion detection systems (IDSs), and other appropriate security measures at each point of entry. Configure firewall rules to prohibit access from and to the critical network, and be as specific as possible when permitting approved connections. For example, an Independent System Operator (ISO) should not be granted "blanket" network access simply because there is a need for a connection to certain components of the critical system. Strategically place IDSs at each entry point to alert security personnel of potential breaches of network security. Organisation management must understand and accept responsibility for risks associated with any connection to the critical network.

2.4 Harden critical networks by removing or disabling unnecessary services.

Critical control servers built on commercial or open-source operating systems can be exposed to attack through default network services. To the greatest degree possible, remove or disable unused services and network daemons to reduce the risk of direct attack. This is particularly important when critical networks are interconnected with other networks. Do not permit a service or feature on a critical

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

network unless a thorough risk assessment of the consequences of allowing the service/feature shows that the benefits of the service/feature far outweigh the potential for vulnerability exploitation. Examples of services to remove from critical networks include automated meter reading/remote billing systems, email services, and Internet access. An example of a feature to disable is remote maintenance. Numerous secure configuration guidelines for both commercial and open source operating systems are available in the public domain. Additionally, work closely with critical vendors to identify secure configurations and coordinate any and all changes to operational systems to ensure that removing or disabling services does not cause downtime, interruption of service, or loss of support.

2.5 Do not rely on proprietary protocols to protect your system.

Some critical systems use unique, proprietary protocols for communications between field devices and servers. Often the security of critical systems is based solely on the secrecy of these protocols. Unfortunately, obscure protocols provide very little "real" security. Do not rely on proprietary protocols or factory default configuration settings to protect your system. Additionally, it may be demanded from vendors to disclose any backdoors or vendor interfaces to your critical systems, and expect them to provide systems that are capable of being secured.

2.6 Implement the security features provided by device and system vendors.

Most older critical systems (most systems in use) have no security features whatsoever. critical system owners must insist that their system vendor implement security features in the form of product patches or upgrades. Some newer critical devices are shipped with basic security features, but these are usually disabled to ensure ease of installation.

Analyse each critical device to determine whether security features are present. Additionally, factory default security settings (such as in computer network firewalls) are often set to provide maximum usability, but minimal security. Set all security features to provide the maximum level of security. Allow settings below maximum security only after a thorough risk assessment of the consequences of reducing the security level.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

329

2.7 Establish strong controls over any medium that is used as a backdoor into the critical network.

Where backdoors or vendor connections do exist in critical systems, strong authentication must be implemented to ensure secure communications. Modems, wireless, and wired networks used for communications and maintenance represent a significant vulnerability to the critical network and remote sites. Successful "war dialing" or "war driving" attacks could allow an attacker to bypass all other controls and have direct access to the critical network or resources. To minimize the risk of such attacks, disable inbound access and replace it with some type of call back system.

2.8 Implementation of control for Data flow

Data diode is a piece of hardware that physically enforces a one-way flow of data. As one-way data transfer systems, data diodes are used as cybersecurity tools to isolate and protect networks from external cyber threats and prevent penetration from any external sources. A data diode sits at the edge of the network security perimeter; relying on its physical hardware components to mitigate all cyber threats against the network while simultaneously allowing the transfer of data out of the network in a highly controlled, deterministic manner. Data diode creates a physical barrier between networks and hence can be used for one-way communication channel from secure network to the insecure network protecting highly sensitive data and networks of critical infrastructure.

2.9 Implement internal and external intrusion detection systems, incident response system and establish 24-hour-a-day incident monitoring.

To be able to effectively respond to cyber-attacks, establish an intrusion detection strategy that includes alerting network administrators of malicious network activity originating from internal or external sources. Intrusion detection system monitoring is essential 24 hours a day. Additionally, incident response procedures must be in place to allow an effective response to any attack. To complement network monitoring, enable logging on all systems and audit system logs daily to detect suspicious activity as soon as possible.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

330

2.10 Perform technical audits of critical devices and networks, and any other connected networks, to identify security concerns.

Technical audits of critical devices and networks are critical to ongoing security effectiveness. Many commercial and open-source security tools are available that allow system administrators to conduct audits of their systems/networks to identify active services, patch level, and common vulnerabilities. The use of these tools will not solve systemic problems, but will eliminate the "paths of least resistance" that an attacker could exploit.

Analyse identified vulnerabilities to determine their significance, and take corrective actions as appropriate. Track corrective actions and analyse this information to identify trends. Additionally, retest systems after corrective actions have been taken to ensure that vulnerabilities were actually eliminated. Scan non-production environments actively to identify and address potential problems.

2.11 Conduct physical security surveys and assess all remote sites connected to the critical network to evaluate their security.

Any location that has a connection to the critical network is a target, especially unmanned or unguarded remote sites. Conduct a physical security survey and inventory access points at each facility that has a connection to the critical system. Identify and assess any source of information including remote telephone/computer network/fiber optic cables that could be tapped; radio and microwave links that are exploitable; computer terminals that could be accessed; and wireless local area network access points. Identify and eliminate single points of failure. The security of the site must be adequate to detect or prevent unauthorized access. Do not allow "live" network access points at remote, unguarded sites simply for convenience.

2.12 Establish critical "Red Teams" to identify and evaluate possible attack scenarios.

Establish a "Red Team (this term refers to teams that conduct security evaluation exercises in an unannounced manner)" to identify potential attack scenarios and evaluate potential system vulnerabilities. Use a variety of people who can provide insight into weaknesses of the overall network, critical systems, physical systems, and security controls. People who work on the system every day have

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

great insight into the vulnerabilities of your critical network and should be consulted when identifying potential attack scenarios and possible consequences. Also, ensure that the risk from a malicious insider is fully evaluated, given that this represents one of the greatest threats to an organisation. Feed information resulting from the "Red Team" evaluation into risk management processes to assess the information and establish appropriate protection strategies.

The following steps focus on management actions to establish an effective cyber security program:

2.13 Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users.

Organisation personnel need to understand the specific expectations associated with protecting information technology resources through the definition of clear and logical roles and responsibilities. In addition, key personnel need to be given sufficient authority to carry out their assigned responsibilities. Too often, good cyber security is left up to the initiative of the individual, which usually leads to inconsistent implementations and ineffective security. Establish cyber security organisational structures that define roles and responsibilities and clearly identify how cyber security issues are escalated and who is notified in an emergency.

2.14 Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection.

Develop and document robust information security architecture as part of a process to establish an effective protection strategy. It is essential that organisations design their networks with security in mind and continue to have a strong understanding of their network architecture throughout its lifecycle. Of particular importance, an in-depth understanding of the functions that the systems perform and the sensitivity of the stored information is required. Without this understanding, risk cannot be properly assessed and protection strategies may not be sufficient. Documenting the information security architecture and its components is critical to understanding the overall protection strategy, and identifying single points of failure.

2.15 Establish a rigorous, ongoing risk management process

A thorough understanding of the risks to network computing resources from denial-of-service attacks and the vulnerability of sensitive information to compromise

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

is essential to an effective cyber security program. Risk assessments form the technical basis of this understanding and are critical to formulating effective strategies to mitigate vulnerabilities and preserve the integrity of computing resources. Initially, perform a baseline risk analysis based on a current threat assessment to use for developing a network protection strategy. Due to rapidly changing technology and the emergence of new threats on a daily basis, an ongoing risk assessment process is also needed so that routine changes can be made to the protection strategy to ensure it remains effective. Fundamental to risk management is identification of residual risk with a network protection strategy in place and acceptance of that risk by management. (Refer ISO 27005)

Legacy technologies are extremely vulnerable to attack from cyber criminals because many of these outdated systems are no longer supported by the manufacturer, a single unpatched vulnerability can enable attackers to access all applications, middleware, and databases running on the server platform. Risk awareness related to legacy technologies need to be maintained and appropriate control should be implemented to reduce the risk. If possible, legacy technologies need to be replaced with the latest technologies to prevent the risk.

2.15.1 Vendor Risk Management

Vendor risk management (VRM) is a comprehensive plan for identifying and decreasing potential business uncertainties and legal liabilities regarding the hiring of 3rd party vendors for information technology (IT) products and services.

Best Practices for Effective Vendor Risk Management:

- Proper planning and due diligence need to be taken for vendor risk identification and mitigation.
- A robust vendor governance program to be developed to assess critical, high, moderate, a nd low risk vendors through surveys and assessments.
- Vendor performance need to be monitored on regular basis to be continually aware of a vendor's capability to comply with contractual obligations. Vendor KPIs and KRIs should be clearly defined in line with applicable laws, regulations, and standards.
- The organisational hierarchy involved in vendor governance need to be defined.

2.15.2 Service Level Agreement (SLA)

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

A Service Level Agreement (SLA) is the service contract component between a service provider and organisation. A SLA provides specific and measurable aspects related to service offerings. For example, SLAs are often included in signed agreements between Internet service providers (ISP) and organisation.

SLAs are an integral part of an IT vendor contract. An SLA pulls together information on all of the contracted services and their agreed-upon expected reliability into a single document. They clearly state metrics, responsibilities and expectations so that, in the event of issues with the service, neither party can plead ignorance. It ensures both sides have the same understanding of requirements.

Any significant contract without an associated SLA (reviewed by legal counsel) is open to deliberate or inadvertent misinterpretation. The SLA protects both parties in the agreement.

2.15.3 Supply Chain Risk Management

Supply chain risk management (SCRM) is the coordinated efforts of an organisation to help identify, monitor, detect and mitigate threats to supply chain continuity and profitability.

The best practices to manage supply chain risks are:

- Include security requirements in every RFP and contract.
- "Right to Audit" on vendor/supplier should be reserved by the organisation and same should be included in the RFP/Contract.
- Trusted source during supply, operation and maintenance phase for products and services need to be ensured
- The cyber security posture of supplier organisation need to be ensured
- After finalization of work contract, involvement of vendor should be there on-site to address any vulnerabilities and security gaps in the supplied products / services.
- Secure Software Lifecycle Development Programs and training for all engineers in the life cycle should be organized.
- Rigorous controls on access by service vendors should be imposed through proper authorization.
- Legacy support for end-of-life products and platforms

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

2.16 Establish a network protection strategy based on the principle of defence-in-depth.

A fundamental principle that must be part of any network protection strategy is defence-in-depth. Defence-in-depth must be considered early in the design phase of the development process, and must be an integral consideration in all technical decision-making associated with the network. Utilize technical and administrative controls to mitigate threats from identified risks to as great a degree as possible at all levels of the network. Single points of failure must be avoided, and cyber security defence must be layered to limit and contain the impact of any security incidents. Additionally, each layer must be protected against other systems at the same layer. For example, to protect against the insider threat, restrict users to access only those resources necessary to perform their job functions.

2.17 Clearly identify cyber security requirements.

Organisations and companies need structured security programs with mandated requirements to establish expectations and allow personnel to be held accountable. Formalized policies and procedures are typically used to establish and institutionalise a cyber-security program. A formal program is essential for establishing a consistent, standards-based approach to cyber security throughout an organisation and eliminates sole dependence on individual initiative. Policies and procedures also inform employees of their specific cyber security responsibilities and the consequences of failing to meet those responsibilities. They also provide guidance regarding actions to be taken during a cyber-security incident and promote efficient and effective actions during a time of cyber crisis. As part of identifying cyber security requirements, include user agreements and notification and warning banners. Establish requirements to minimize the threat from malicious insiders, including the need for conducting background checks and limiting network privileges to those absolutely necessary.

2.18 Establish effective configuration management processes.

A fundamental management process needed to maintain a secure network is configuration management. Configuration management needs to cover both

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

hardware configurations and software configurations. Changes to hardware or software can easily introduce vulnerabilities that undermine network security. Processes are required to evaluate and control any change to ensure that the network remains secure. Configuration management begins with well-tested and documented security baselines for your various systems.

2.19 Conduct routine self-assessments.

Robust performance evaluation processes are needed to provide organisations with feedback on the effectiveness of cyber security policy and technical implementation. A sign of a mature organisation is one that is able to self-identify issues, conduct root cause analyses, and implement effective corrective actions that address individual and systemic problems. Self-assessment processes that are normally part of an effective cyber security program include routine scanning for vulnerabilities, automated auditing of the network, and self-assessments of organisational and individual performance.

2.20 Establish system backups and disaster recovery plans.

Establish a disaster recovery plan that allows for rapid recovery from any emergency (including a cyber attack). System backups are an essential part of any plan and allow rapid reconstruction of the network. Routinely exercise disaster recovery plans to ensure that they work and that personnel are familiar with them. Make appropriate changes to disaster recovery plans based on lessons learned from exercises.

2.21 Senior organisational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance.

Effective cyber security performance requires commitment and leadership from senior managers in the organisation. It is essential that senior management establish an expectation for strong cyber security and communicate this to their subordinate managers throughout the organisation. It is also essential that senior organisational leadership establish a structure for implementation of a cyber-security program. This structure will promote consistent implementation and the ability to sustain a strong cyber security program. It is then important for individuals to be held accountable for their performance as it relates to cyber security. This includes managers, system administrators, technicians, and users/operators.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

2.22 Establish policies and conduct training to minimize the likelihood that organisational personnel will inadvertently disclose sensitive information regarding critical system design, operations, or security controls.

Release data related to the critical network only on a strict, need-to-know basis, and only to persons explicitly authorized to receive such information. "Social engineering," the gathering of information about a computer or computer network via questions to naive users, is often the first step in a malicious attack on computer networks. The more information revealed about a computer or computer network, the more vulnerable the computer/network is. Never divulge data related to a critical network, including the names and contact information about the system operators/administrators, computer operating systems, and/or physical and logical locations of computers and network systems over telephones or to personnel unless they are explicitly authorized to receive such information. Any requests for information by unknown persons need to be sent to a central network security location for verification and fulfilment. People can be a weak link in an otherwise secure network. Conduct training and information awareness campaigns to ensure that personnel remain diligent in guarding sensitive network information, particularly their passwords.

3.0 Guidelines on Cyber Crisis Management plan for critical networks

3.1 Strategic issues in cyber crisis management and business continuity

- Implementation of appropriate measures to reduce the likelihood of incidents occurring and/or reduce the potential effects of those incidents
- Taking due account of the resilience and mitigation measures
- Providing continuity for critical services during and following an incident
- Taking into account those activities that have not been identified as critical

The effectiveness of above actions depends on a range of factors such as:

- The maximum tolerable period of disruption of a critical activity
- The costs of implementing a strategy and
- Consequences of inaction

3.2 Effective cyber crisis management and business continuity strategies also cover the following:

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

3.2.1 People

Organisations should identify appropriate strategies for maintaining core skills and knowledge. This analysis should go beyond employees to contractors and other stakeholders who possess extensive specialist skills and knowledge. Strategies to protect or provide those skills might include:

- Documentation of the way in which critical activities are performed
- Multi-skill training of staff and contractors
- Separation of core skills to reduce the concentration of risk
- Use of third parties
- Succession planning and
- Knowledge retention and management

3.2.2 Premises

Organisations should devise a strategy for reducing impact of unavailability of its normal work site(s). This may include one or more of the following:

- Alternative premises (locations) within the organisation including displacement of other activities
- Alternative sites provided by other organisations
- Alternative premises provided by third party specialists
- Working from home or at remote sites
- Other agreed suitable premises and
- Use of an alternative workforce in an established site

3.2.3 Technology

Technology strategies depend on the nature of the technology employed and its relationship with critical activities, but will typically be one or a combination of the following:

- Provision made within the organisation
- Services delivered to the organisation and
- Services provided externally by a third party

Technology strategies may include:

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

- Geographical spread of technology
- Holding older equipment as emergency replacement or spares and '
- Additional risk mitigation for unique or long lead time equipment

Information technology (IT) services require complex continuity strategies. In such cases, consideration should be given to:

- Recovery time objectives (RTO) for systems and applications that support the key activities identified in the business impact analysis
- Location and distance between technology sites
- Number of technology sites
- Remote access
- Use of un-staffed sites as opposed to staffed sites
- Telecom connectivity and redundant routing
- The nature of fail-over (whether manual intervention is required to activate alternative IT provision or it can be done automatically)
- Third party connectivity and external links

3.2.4 Information

Information strategies should be such as to ensure that information vital to the organisation's operation is protected and recoverable according to the time frames prescribed with the business impact analysis. These strategies should include information in both hard copy formats and electronic formats. Any information required for enabling the delivery of organisation's critical activities should have appropriate:

- Confidentiality
- Integrity
- Availability and
- Currency

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Appendix – VII Sample Business Impact Analysis (BIA)

Business Impact Analysis (BIA) as applied to a small organisation / field office

In this example, an agency maintains a small field office with a local area network (LAN) that supports about 50 users. The office relies on the LAN and its components for standard automated processes, such as developing and using spreadsheets, word processing, and electronic mail (e-mail). The office also maintains a customized database application that supports Inventory, a key resource management process. The network manager is responsible for developing a LAN contingency plan and begins with the business impact analysis (BIA). The LAN includes the following components:

- Authentication/network operating system server
- Database server (supports customized Inventory database application)
- File server (stores general, non-Inventory files)
- Application server (supports office automation software)
- Networked printer
- E-mail server and application
- 50 desktop computers
- Five hubs.

The Contingency Planning Coordinator begins the BIA process by identifying the network stakeholders. In this case, the coordinator identifies and consults with the following individuals:

- Field office manager
- Inventory process manager
- Sampling of network users
- System administrators for each network server.

Based on subsequent discussions, the coordinator learns the following information:

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

- The Inventory system is critical to the parent agency's master resource management operations; the system provides updated data to the larger system at the end of each business day. If the system were unavailable for more than 1 working day (8 hours), significant business impacts would result at the parent agency. Inventory requires a minimum of five personnel with desktop computers and access to the system database to process data.
- Other non-Inventory processes may be considered non-critical and could be allowed to lapse for up to 10 days.
- The field office manager and Inventory manager indicate that e-mail is an essential service; however, staff can operate effectively without e-mail access for up to 3 days.
- Staff could function without access to the spreadsheet application for up to 15 working days without affecting business processes significantly.
- Word processing access would need to be restored within 5 working days; however, individuals could use manual processes for up to 10 days if the required forms were available in hard-copy format.
- Outputs from the day's Inventory system records normally are printed daily; the data to be printed may be stored on any desktop computer used by the Inventory system staff. In an emergency, the Inventory system output could be transmitted electronically via e-mail for up to 3 days before significantly affecting business operations. Other printing functions would not be considered essential and could be unavailable for up to 10 days with no impact on business functions.

Based on the information gathered in discussions with stakeholders, the Contingency Planning Coordinator follows the three-step BIA process to identify critical information technology (IT) resources, identify outage impacts and allowable outage times, and develop recovery priorities.

Identify Critical IT Resources

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

The manager identifies the following resources as critical, meaning that they support critical business processes:

- Authentication/network operating system server (required for users to have LAN access)
- Database server (required to process the Inventory system)
- E-mail server and application
- Five desktop computers (to support five Inventory users)
- One hub (to support five Inventory users)
- Network cabling
- Electric power
- Heating, ventilation, and air conditioning (HVAC)
- Physical security
- Facility.

Identify Outage Impacts and Allowable Outage Times

Next, the manager determines outage impacts and allowable outage times for the critical resources:

Resource	Outage Impact	Allowable Outage Time
Authentication server	Users could not access Inventory system	8 hours
Database server	Users could not access Inventory system	8 hours
E-mail server	Users could not send e-mail	2 days
5 desktop computers	Users could not access Inventory system	8 hours
Hub	Users could not access Inventory system	8 hours
Network cabling	Users could not access Inventory system	8 hours
Electric power	Users could not access Inventory system	8 hours
Printer	Users could not produce Inventory reports	4 days

Develop Recovery Priorities

Using the table completed in the previous step, the Contingency Planning Coordinator develops recovery priorities for the system resources. The manager uses a simple high-, medium-, low-scale to prioritize the resources. High priorities are based on the need to restore critical resources within their allowable outage times; medium and low priorities reflect the requirement to restore full operational capabilities over a longer recovery period.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Resource	Recovery Priority
Authentication server	High
Database server	High
5 desktop computers	High
1 hub	High
Network cabling	High
Electric power	High
E-mail server	Medium
Printer	Medium
Remaining desktop computers (45)	Low
Remaining hubs (4)	Low

Having completed the BIA, the Contingency Planning Coordinator may use the recovery priority information above to develop strategies that enable all system resources to be recovered within their respective allowable outage times and in a prioritized manner.

A template for completing the BIA is provided below.

Business Impact Analysis (BIA) Template

This sample template is designed to assist the user in performing a BIA on an IT system. The BIA is an essential step in developing the IT contingency plan. The template is meant only as a basic guide and may not apply to all systems. The user may modify this template or the general BIA approach as required to best accommodate the specific system.

Preliminary System Information Organisation: Date BIA Completed:

System Name: BIA POC:

System Manager Point of Contact (POC):

System Description: {Discussion of the system purpose and architecture, including system diagrams}

A. Identify System POCs Role

Internal POC {Identify the individuals, positions, or offices within your organisation that

depend on or support the system; also specify their relationship to the system}

- XXXX
- XXXX
- XXXX
- XXXX
- XXXX
- XXXX

External POC {Identify the individuals, positions, or offices outside your organisation that depend on or support the system; also specify their relationship to the system}

- XXXX
- XXXX
- XXXX
- XXXX
- XXXX
- XXXX

B. Identify System Resources {Identify the specific hardware, software, and other resources that comprise the system; include quantity and type}

Hardware

- XXXX
- XXXX
- XXXX

Software

- XXXX
- XXXX
- XXXX

Other resources

- XXXX
- XXXX
- XXXX

C. Identify critical roles {List the roles identified in Section A that are deemed critical}

- XXXX
- XXXX
- XXXX

D. Link critical roles to critical resources {Identify the IT resources needed to accomplish the roles listed in Section C}

Critical Role **Critical Resources**

- XXXX
- XXXX
- XXXX
- XXXX

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

- XXXX
- XXXX

- XXXX
- XXXX
- XXXX

E. Identify outage impacts and allowable outage times {Characterize the impact on critical roles if a critical resource is unavailable; also, identify the maximum acceptable period that the resource could be unavailable before unacceptable impacts resulted}

Resource	Outage Impact	Allowable Outage Time
	• XXXX • XXXX • XXXX	• XXXX • XXXX • XXXX
	• XXXX • XXXX • XXXX	• XXXX • XXXX • XXXX • XXXX
	• XXXX • XXXX • XXXX	• XXXX • XXXX • XXXX

F. Prioritize resource recovery {List the priority associated with recovering a specific resource, based on the outage impacts and allowable outage times provided in Section E. Use quantitative or qualitative scale (e.g., high/medium/low, 1-5, A/B/C)}

Resource	Recovery Priority

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Appendix – VIII IT Contingency Plan template for use by Critical Sector organisations

1. INTRODUCTION

1.1 PURPOSE

This {system name} Contingency Plan establishes procedures to recover the {system name} following a disruption. The following objectives have been established for this plan:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:

  – **Notification/Activation phase** to detect and assess damage and to activate the plan

  – **Recovery phase** to restore temporary IT operations and recover damage done to the original system

  – **Reconstitution phase** to restore IT system processing capabilities to normal operations.

- Identify the activities, resources, and procedures needed to carry out {system name} processing requirements during prolonged interruptions to normal operations.

- Assign responsibilities to designated {Organisation name} personnel and provide guidance for recovering {system name} during prolonged periods of interruption to normal operations.

- Ensure coordination with other {Organisation name} staff who will participate in the contingency planning strategies. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

1.2 APPLICABILITY

The {system name} Contingency Plan applies to the functions, operations, and resources necessary to restore and resume {Organisation name}'s {system name}

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

operations as it is installed at primary location name, City, State. The {system name} Contingency Plan applies to {Organisation name} and all other persons associated with {system name} as identified under Section 2.3, Responsibilities.

The {system name} Contingency Plan is supported by plan name, which provides the purpose of plan. Procedures outlined in this plan are coordinated with and support the plan name, which provides purpose of plan.

1.3 SCOPE

1.3.1 Planning Principles

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on two key principles:

- The {Organisation name}'s facility in City, State, is inaccessible; therefore, {Organisation name} is unable to perform {system name} processing for the Department.
- A valid contract exists with the alternate site that designates that site in City, State, as the {Organisation name}'s alternate operating facility.
  - {Organisation name} will use the alternate site building and IT resources to recover {system name} functionality during an emergency situation that prevents access to the original facility.
  - The designated computer system at the alternate site has been configured to begin processing {system name} information.
  - The alternate site will be used to continue {system name} recovery and processing throughout the period of disruption, until the return to normal operations.

1.3.2 Assumptions

Based on these principles, the following assumptions were used when developing the IT Contingency Plan:

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

347

- The {system name} is inoperable at the {Organisation name} computer center and cannot be recovered within 48 hours.
- Key {system name} personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the {system name} Contingency Plan.
- Preventive controls (e.g., generators, environmental controls, waterproof tarps, sprinkler systems, fire extinguishers, and fire department assistance) are fully operational at the time of the disaster.
- Computer center equipment, including components supporting {system name}, are connected to an uninterruptible power supply (UPS) that provides 45 minutes to 1 hour of electricity during a power failure.
- {system name} hardware and software at the {Organisation name} original site are unavailable for at least 48 hours.
- Current backups of the application software and data are intact and available at the offsite storage facility.
- The equipment, connections, and capabilities required to operate {system name} are available at the alternate site in City, State.
- Service agreements are maintained with {system name} hardware, software, and communications providers to support the emergency system recovery.

1.4 REFERENCES/REQUIREMENTS

This {system name} Contingency Plan complies with the {Organisation name}'s IT contingency planning policy as follows:

> The organisation shall develop a contingency planning capability to meet the needs of critical supporting operations in the event of a disruption extending beyond 72 hours. The procedures for execution of such a capability shall be documented in a formal contingency plan and shall be reviewed at least annually and updated as necessary. Personnel responsible for target systems shall be trained to execute contingency procedures. The plan, recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

The {system name} Contingency Plan is in line with the following National policies:

- National Cyber Security Strategy, DIT Govt. of India
- National Information Security Policy, Version 1, May 06
- Cyber Crisis management Plan for countering cyber attacks and cyber terrorism
- [Add any other applicable National policies]
- [Add any other applicable departmental policies]

1.5 RECORD OF CHANGES

Modifications made to this plan since the last printing are as follows: **Record of Changes**

Page No.	Change Comment	Date of Change	Signature

2. CONCEPT OF OPERATIONS

2.1 SYSTEM DESCRIPTION AND ARCHITECTURE

<Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organisations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures.>

<Provide a diagram of the architecture, including security controls and telecommunications connections.>

2.2 LINE OF SUCCESSION

The {organisation name} sets forth an order of succession, in coordination with the order set forth by the department to ensure that decision-making authority for the {system name} Contingency Plan is uninterrupted. The Chief Information Officer (CIO), {organisation name} is responsible for ensuring the safety of personnel and

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

the execution of procedures documented within this {system name} Contingency Plan. If the CIO is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Deputy CIO shall function as that authority. Continue description of succession as applicable.

2.3 RESPONSIBILITIES

The following teams have been developed and trained to respond to a contingency event affecting the IT system.

The Contingency Plan establishes several teams assigned to participate in recovering {system name} operations.

- The {team name} is responsible for recovery of the {system name} computer environment and all applications. Members of the team name include personnel who are also responsible for the daily operations and maintenance of {system name}. The team leader {title} directs the {team name}.
- [Continue to describe each team, their responsibilities, leadership, and coordination with other applicable teams during a recovery operation]

<Describe each team separately, highlighting overall recovery goals and specific responsibilities. Do not detail the procedures that will be used to execute these responsibilities. These procedures will be itemized in the appropriate phase sections.>

The relationships of the team leaders involved in system recovery and their member teams are illustrated in Figure XX below.

[Insert hierarchical diagram of recovery teams. Show team names and leaders; do not include actual names of personnel]

3. NOTIFICATION AND ACTIVATION PHASE

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

350

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to {system name}. Based on the assessment of the event, the plan may be activated by the Contingency Planning Coordinator.

In an emergency, the {Organisation name}'s top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.

Contact information for key personnel is located in Annexure I. The notification sequence is listed below:

- The first responder is to notify the Contingency Planning Coordinator. All known information must be relayed to the Contingency Planning Coordinator.
- The systems manager is to contact the Damage Assessment Team Leader and inform them of the event. The Contingency Planning Coordinator is to instruct the Team Leader to begin assessment procedures.
- The Damage Assessment Team Leader is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the Damage Assessment Team is to follow the outline below.

Damage Assessment Procedures:

(Detailed procedures should be outlined to include activities to determine the cause of the disruption; potential for additional disruption or damage; affected physical area and status of physical infrastructure; status of IT equipment functionality and inventory, including items that will need to be replaced; and estimated time to repair services to normal operations.)

- Upon notification from the Contingency Planning Coordinator, the Damage Assessment Team Leader is to …
- The Damage Assessment Team is to ….

Alternate Assessment Procedures:

- Upon notification from the Contingency Planning Coordinator, the Damage Assessment Team Leader is to …
- The Damage Assessment Team is to ….

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

351

- When damage assessment has been completed, the Damage Assessment Team Leader is to notify the Contingency Planning Coordinator of the results.
- The Contingency Planning Coordinator is to evaluate the results and determine whether the contingency plan is to be activated and if relocation is required.
- Based on assessment results, the Contingency Planning Coordinator is to notify assessment results to civil emergency personnel (e.g., police, fire) as appropriate.

The Contingency Plan is to be activated if one or more of the following criteria are met:

1. {System name} will be unavailable for more than 48 hours
2. Facility is damaged and will be unavailable for more than 24 hours
3. Other criteria, as appropriate.

- If the plan is to be activated, the Contingency Planning Coordinator is to notify all Team Leaders and inform them of the details of the event and if relocation is required.
- Upon notification from the Contingency Planning Coordinator, Team Leaders are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.
- The Contingency Planning Coordinator is to notify the off-site storage facility that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.
- The Contingency Planning Coordinator is to notify the Alternate site that a contingency event has been declared and to prepare the facility for the Organisation's arrival.
- The Contingency Planning Coordinator is to notify remaining personnel (via notification procedures) on the general status of the incident.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

4. RECOVERY OPERATIONS

This section provides procedures for recovering the application at the alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

The following procedures are for recovering the {system name} at the alternate site. Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal. State the first recovery objective as determined by the Business Impact Assessment (BIA). For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.

- {team name}
  - Team Recovery Procedures
- {team name}
  - Team Recovery Procedures
- {team name}
  - Team Recovery Procedures

Recovery Goal. State the second recovery objective as determined by the BIA. For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.

- {team name}
  - Team Recovery Procedures
- {team name}
  - Team Recovery Procedures
- {team name}
  - Team Recovery Procedures

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Recovery Goal. [State the remaining recovery objectives (as determined by the BIA). For each team responsible for executing a function to meet this objective, state the team names and list their respective procedures.]

5. RETURN TO NORMAL OPERATIONS

This section discusses activities necessary for restoring {system name} operations at the {Organisation name}'s original or new site. When the computer center at the original or new site has been restored, {system name} operations at the alternate site must be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

Original or New Site Restoration

Procedures should be outlined, per necessary team, to restore or replace the original site so that normal operations may be transferred. IT equipment and telecommunications connections should be tested.

- {team name}

  – Team Resumption Procedures

- {team name}

  `– Team Resumption Procedures

5.1 CONCURRENT PROCESSING

Procedures should be outlined, per necessary team, to operate the system in coordination with the system at the original or new site. These procedures should include testing the original or new system until it is functioning properly and the contingency system is shut down gracefully.

- {team name}

  – Team Resumption Procedures

- {team name}

  – Team Resumption Procedures

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

5.2 PLAN DEACTIVATION

Procedures should be outlined, per necessary team, to clean the alternate site of any equipment or other materials belonging to the organisation, with a focus on handling sensitive information. Materials, equipment, and backup media should be properly packaged, labeled, and shipped to the appropriate location(s). Team members should be instructed to return to the original or new site.

- {team name}

  – Team Testing Procedures

- {team name}

  – Team Testing Procedures

6. PLAN APPENDICES

The appendices included should be based on system and plan requirements.

- Personnel Contact List
- Vendor Contact List
- Equipment and Specifications
- Service Level Agreements and Memorandums of Understanding
- IT Standard Operating Procedures
- Business Impact Analysis
- Related Contingency Plans
- Emergency Management Plan
- Occupant Evacuation Plan
- Business Continuity Plan.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Appendix – IX Points of Action for preparation Cyber Crisis Management Plans

I. Sectoral Cyber Crisis Management Plans

The critical sectors and governments of states and Union Territories are required to prepare the Sectoral Cyber Crisis Management Plans in line with this Cyber Crisis Management Plan.

The following are the set of actions required for preparing the sectoral CMPs:

1. Identify a member of senior management as a **'Point of Contact'** to coordinate security policy compliance efforts across the sector and interact regularly with CERT-In
2. Establish a **Sectoral Crisis Management Committee**, on the lines of National Crisis Management Committee, with Secretary *(in case of Central Ministries/Depts)* or Chief Secretary *(in case of States/UTs)* as its Chairman and a **24x7 control room** to monitor crisis situations
3. Prepare a **list of organisational units** that fall under the purview of sectoral CMP and provide them with a **list of action points** for compliance
4. Direct the organisational units to identify and designate a member of senior management as **'Chief Information Security Officer (CISO)'**
5. Prepare a **list of CISOs** complete with up-to-date contact details
6. Prepare a **sectoral CMP** on the lines of CMP of CERT-In, outlining roles, responsibilities of sectoral stakeholders, CMP coordination process
7. Direct the organisational units to **develop and implement their own CMP** on the lines of CMP of CERT-In, including security best practices as per ISO 27001 and **report compliance** on a periodic basis
8. Participate in the cyber security exercises to be conducted by CERT-In on a regular basis

II. Organisational Cyber Crisis Management Plans

1 Identify a member of senior management as a **'Chief Information Security Officer (CISO)'** to coordinate security policy compliance efforts across the organisation and interact regularly with CERT-In and sectoral 'Point of Contact'

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

2 Establish a Crisis Management Group, on the lines of Sectoral Crisis Management Committee, with head of organisation as its Chairman

3 Prepare a list of contact persons complete with up-to-date contact details

4 Prepare an Organisational level CMP on the lines of CMP of CERT-In, outlining roles, responsibilities of organisational stakeholders, CMP coordination process

5 Implement the CMP, including security best practices and specific action points as outlined below:

- Prepare a **Security plan** and implement Security control measures as per **ISO 27001 standard** and other guidelines/standards as appropriate
- Carry out **periodic IT security risk assessments** and determine acceptable level of risks, consistent with business impact assessment and criticality of business functions
- Develop and implement a **business continuity strategy** and **contingency plan** for IT systems
- Develop and implement **ICT disaster recovery** and **security incident management processes**
- **Periodically test and evaluate** the adequacy and effectiveness of technical security control measures, especially after each significant change to the IT applications/systems/networks and it can include:
  - *i.* Penetration testing *(both announced and unannounced)*
  - ii. Vulnerability assessment
  - iii. Application security testing
  - iv. Web security testing
  - *v.* Carry out **audit of information infrastructure and applications** on an annual basis and when there is a major upgradation/change in IT infrastructure/application, by an independent IT security auditing organisation *(Ref. to list of CERT-In empanelled IT security auditing organisations on CERT-In web site at http://www.cert-in.org.in)*

6 Report to CERT-In cyber security incidents as and when they occur. Also inform status of cyber security assurance level periodically to respective administrative ministry / sectoral CSIRTs.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Participate in the cyber security exercises to be conducted by CERT-In on a regular basis

115

Appendix – X Cyber Resilience Control matrix

Component	Protect	Detect	Contain	Recover
Identity	• Controlled access based on need-to-know • Enforce Strong password policy • Multi factor authentication • Usage of Digital Certificates	• Maintenance and Analysis of complete security events and audit logs • Privilege escalation monitoring and alerting	• Minimize the invalid logon counts • Revocation of digital certificate • Change access control on all devices • Continuous account monitoring and deactivating the dormant accounts	• Offline recovery procedures for logging into accounts • Alternative Indicators
System Processes	• Effective Security Patch Updating Mechanism on applications etc. • Following Best Security practices during Software Development Lifecycle • Secure configuration • Malware defenses	• Forensic Memory Analysis • File integrity checking • Malware Analysis	• Policy based restrictions on process actions • Reconfiguration of settings • Usage of Sandbox Security Mechanism	• Assured Data Back-ups • Clustering • Recovery Time Objectives (RTO) for system and support • Manual /automated takeover to activate alternative IT provision • Use of Unstaffed sites as opposed to staffed sites
Hardware and Software Platform	• Asset Inventory (asset classification and management) • Supply chain protections	• Continuous vulnerability testing and remediation • Tamper detection mechanism • Platform Security Assessment (	• Remote Wipe on failed logins • Code Integrity Checks to help prevent malicious code from being injected into system files or	• Baseline remote image deployment • Usage of Virtual environment • Assured Back-up and replication

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

	• Regular review of configuration files : OS/middleware • Boot process integrity check	Review of System architecture/Operating system configuration/Security management controls/System configuration)	into the kernel at load/run time	• Replacing compromised files with clean versions
Data	• Database access control: Regular review of access privileges to users of the database/use of biometric technology • Data Encryption while in-process, handling, storage or transit) • Data Masking (for sensitive information) •	• Monitoring Data flow to detect data leakage • Forensic disk imaging and analysis • Monitoring remote access • Database integrity Checking	• Application restrictions monitoring • Data Leakage Prevention (system designed to detect potential data leakage while in-process, handling, storage or transit • Access Control on Database	• Assured Data Back-ups and physical segregation of back-up • Storage replication Mirroring/Cloning • Database reprocessing(Going back to a known point of database activity before the problem occurred and reprocessing work from that point forward)
Network	• Limitation and control of ports, protocols and services • Wireless Device Control • Following Best Practices for secure configuration of network devices •	• Centralised network log analysis for wired & wireless networks • Honey-net • Network Scanning and Analysis •	• Isolation of trusted networks from untrusted networks. • Denial of service offload to ISP and cloud • Reconfiguration of impacted network devices • Modify access control (all user/root/administrator passwords) in all systems and network devices	• Alternate network routing • Alternative cloud communications • Usage of devices in cluster mode/load balancing mode

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

360

References

[1] Building Cyber Resilience-Microsoft Whitepaper

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Appendix – XI IT Security best practices Compliance and Assurance – 'Levels of Assurance'

Sl No	Assurance Level	Description	Methods of verification
1	**Level 1 – Assurance of systematic approach to IT Security**	Organisation is **aware of IT security best practices** and has **defined and documented** its IT security plan, policies and procedures covering people, products, technology and processes. Evidence in the form of appropriate references to the IT security plan, policies and procedures exists.	• Questionnaire based check-list and • Remote or on-site desk-top assessment of check-list response
2	**Level 2 – Assurance of compliance to IT security best practices**	Organisation has **implemented IT security best practices** based on clear understanding of risks, threats & vulnerabilities and the **compliance has been verified** by a self-assessment process or by an independent third party auditing organisation.	• Self-assessment report or independent third party audit report
3	**Level 3 – Assurance of an adequate IT security posture**	Organisation has **conducted IT security posture verification** (by way of security testing of its IT infrastructure involving VA/PT, application security testing, code walk-throughs etc) by an independent third party auditing organisation.	• Security testing of of web / mobile application, IT infrastructure involving VA/PT, application security testing, code walk-throughs etc and a report is available for the same.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

		Organisation has formed Incident response group with roles and responsibilities clearly assigned to different members, properly defined escalation matrix	• Composition of Incident response group
		Cyber Crisis Management Plan (CCMP) document has been developed and implemented within the organisation	• Details of implementation / revision (if any) of CCMP
	Level 3+ - Assurance of IT security crisis response & ability to resist cyber attacks	Organisation has **participated in the cyber security exercise** to have its IT security crisis response & ability to resist cyber attacks tested and verified	• Result of Cyber security exercise with CERT-In
4	**Level 4 – Assurance of proactive IT security monitoring and mitigation of threats and vulnerabilities**	Organisation has **implemented mechanisms for proactive IT security monitoring and mitigation** of threats and vulnerabilities. These mechanisms allow for technology based monitoring and analysis of IT security incidents for proactive preventive actions (Ex. IPS/IDS, SIEM, flow based analysis etc).	• Technology based monitoring and analysis (Ex. IPS/IDS, SIEM, flow based analysis etc) evidenced in terms of governance reports and management feedback
	Level 4+ - Assurance of proactive sharing	Organisation has **implemented mechanisms for proactive sharing and**	• Collaboration with CERT-In, sectoral

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

	and mitigation of IT security threats & vulnerabilities.	**mitigation** of IT security threats & vulnerabilities by way of active collaboration with CERT-In, sectoral CERTs, ISACs etc	CERTs, ISACs etc evidence in terms of communication trail
	Level 4+ + - Assurance of proactive prediction of residual IT security risks & attack paths and mitigation	Organisation has **implemented mechanisms for proactive prediction of residual IT security risks & attack paths** and mitigation of upcoming cyber security threats and vulnerabilities.	• Attack path analysis

Appendix XII Nature and Severity of cyber crisis

<Modify the Tables A 12.1 below suitably to reflect your situation>

Table A12.1: Nature and Severity of cyber crisis, Authorities responsible and steps for mitigation

Severity Level of cyber Crisis	Nature of cyber Crisis	Authorities responsible and Steps for mitigation
Level 1 Response Scope: Individual Organisation	All attacks	**Responsibility: <Mention name of Affected Organisation >** **Steps to be taken by the Affected Organisations** **General** • Notify incidents to respective administrative Ministry/Department • Monitor and detect anomalous behavior and degradation of service in network and systems • Take all logs (system, application, security, access, error etc) of affected systems and data therein and keep them separately for analysis and forensics • Forward a copy of all the logs of affected systems and network devices, suspicious files, data, traffic trends wherever applicable to CERT-In/NTRO/MoD, IDS (DIARA) • Consult incident reports or vulnerability reports for specific advisories on the suspected behaviour as published by CERT-In and implement those in the affected networks and systems • Segregate networks (LAN/WAN) and perimeter security devices and systems. Check for configuration vis-à-vis ongoing attack. Implement the appropriate eradication process and recovery of system files and data as prescribed against each attacks mentioned below. • Change all user/root/administrator passwords in all systems and network devices • Install updated software patches on Operating System and all other system software running on computer servers and Personal computers in the network **Mitigation Steps - Specific to nature of cyber attacks/crisis**

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

	Webapplication attacks	• If possible, Isolate affected server from Internet or disable the affected module in application. • Scan all files for webshells or any malicious footprint. • Take a copy of all the logs at the server and perimeter level (IDS/IPS, firewall) and traffic trends • Identify the type of attack and vulnerability exploited • Patch the vulnerability/ issue by modifying insecure code/configuration by secure code/configuration • Report to CERT-In with web server logs and dump of the vulnerable web application
	Virus/Worm/Spyware/Botnet attacks	• Isolate affected systems/network segments from LAN and Internet • Scan all files in the suspected systems, including emails for viruses. • Clean the affected systems with the updated antivirus software. • Install updated Antivirus/anti-spyware on all systems (servers and Personal Computers)
	DoS/DDoS attacks/NTP based DrDoS attacks	• Take a copy of all the logs at the perimeter level (IDS/IPS, firewall) and traffic trends • Identify the type of attack such as flooding of particular types of packets/requests • Allocate traffic to unaffected available network paths, if possible, to continue the services • Apply appropriate rate limiting strategies at the local perimeter and if necessary consult ISP • Implement Egress and Ingress filtering to block spoofed packets • Use appropriate DoS prevention tools • Install updated software patches on all the network devices such as Routers, Firewalls, IDS, IPS and switches.
	High Energy RF-based DoS Attacks	• Use a network management solution capable of alerting on a degraded signal noise ratio or the increased noise levels in the airwaves. • Identify the other devices due to which RF interference occurs and physically remove them. • Deploy IPS/IDS to detect rouge access points
	DNS Attack	• Check for version updates at the DNS server and install latest software patches • Implement spoofing countermeasures • Use Unicast Reverse Path Forwarding to mitigate problems that are caused by malformed or forged IP source addresses

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

		• Adopt source IP address verification • Implement DNSSec
	Attack attempts/scans on Servers, Routers, Firewall etc.	• Check for effectiveness of filtering rules in the routers, firewall and IPS and reconfigure if required. • Check the logs of these devices for source of attack.
	Phishing attacks	• Keep watch on phishing sites • Alert customers regarding the known phishing sites • Encourage customers to use anti-phishing enabled browsers • Shutdown phishing sites in coordination with concerned ISP and CERT-In
	Mail Server attacks	• Deploy hot standby mail servers in physically separated networks and places which can be made operational when the main server is attacked • Disable all other ports and services on mail servers • Enforce strong password policy and encourage users to change passwords periodically
	Attacks on Critical Infrastructure and associated SCADA/ Industrial Control Systems, through sophisticated malware such as Stuxnet/Duqu/Nitro/ Flame	• Check for signs of infection in computer systems in general • Isolate infected systems from all networks immediately • Report the incident to local IR Team/CERT-In at the earliest. Consult relevant advisories of CERT-In and follow specific measures suggested therein • Take a forensic image and send to local IR Team/CERT-In • Clean the affected systems with the updated antivirus software. • Install updated Antivirus/anti-spyware on all systems (servers and Personal Computers) • Examine the vectors of propagation of worms – Removal media, network shares and other sneakernet systems. • Examine the critical SCADA/Industrial Control Systems/PLCs for abnormal functionality • Examine Critical systems of Industrial process for abnormal functionality • Examine network traffic towards malicious domains/websites/hosts that are indentified as Command & Control • Trace the infected PLCs/Systems and isolate immediately. • Review the security controls and processes to ensure isolation of critical networks from other infrastructure • Follow guidelines mentioned under Appendix VI in respect of dealing with air gap for isolation of control systems from

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

		other networks
		On report of the incident, CERT-In would take following supportive actions • Analyse the information/logs received from affected organisations. • Check for latest patches/updates from various sources including vendors • Consult the vendors and other sources to help the organisations in resolving the problems • Document the vulnerability information and disseminate. • In case of phishing attacks, take appropriate action to block the phishing sites by interfacing with concerned organisations, ISPs and international CERTs • In case of Botnet attacks, locate Command & Control server and initiate action to disable the same in coordination with ISPs

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Level 2 Response **Scope:** **Multiple Organisations**		**Responsibility:** ***< Mention Name of Respective Central Ministry/Department/State/UT >*** **Steps to be taken by affected Organisations** **General**
	All attacks	• Notify incidents to respective administrative Ministry/Department • Monitor and detect anomalous behavior and degradation of service in network and systems • Take all logs (system, application, security, access, error etc) of affected systems and data therein and keep them separately for analysis and forensics • Forward a copy of all the logs of affected systems and network devices, suspicious files, data, traffic trends wherever applicable to CERT-In/NTRO/MoD, IDS (DIARA) • Consult incident reports or vulnerability reports for specific advisories on the suspected behaviour as published by CERT-In and implement those in the affected networks and systems • Segregate networks (LAN/WAN) and perimeter security devices and systems. Check for configuration vis-à-vis ongoing attack. Implement the appropriate eradication process and recovery of system files and data as prescribed against each attacks mentioned below. • Change all user/root/administrator passwords in all systems and network devices
		Mitigation Steps - Specific to nature of cyber attacks/crisis
	Webapplication	• if possible, Isolate affected server from Internet or disable the affected module in application. • Scan all files for webshells or any malicious footprint. • Take a copy of all the logs at the server and perimeter level (IDS/IPS, firewall) and traffic trends • Identify the type of attack and vulnerability exploited • Patch the vulnerability/ issue by modifying insecure code/configuration by secure code/configuration • Report to CERT-In with webserver logs and dump of the vulnerable web application

126

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

	Virus/Worm/Spyware/Botnet attacks	• Isolate affected systems/network segments from LAN/Internet • Scan all files in the suspected systems, including emails for viruses • Install Antivirus/anti-spyware updates • Clean the affected systems with the updated antivirus software • Block the infection/attack vectors through IPS/Firewall
	DoS/DDoS attacks/ NTP Based DrDoS attacks	• Shift critical services to alternate channels. • Incase of IP based attacks, shift hosting of affected services to different ISPs. • Apply appropriate rate limiting strategies at the local perimeter and if necessary consult ISP • Implement Egress and Ingress filtering to block spoofed packets • Use appropriate DoS prevention tools • Take a copy of all the logs at the perimeter level (IDS/IPS, firewall) and traffic trends • Install updated patches on the network devices
	High Energy RF-based DoS Attacks	• Use a network management solution capable of alerting on a degraded signal noise ratio or the increased noise levels in the airwaves. • Identify the other devices due to which RF interference occurs and physically remove them. • Relocate the Access Points incase of Wireless Networks
	DNS Attack	• Change the preferred DNS server • Implement Source address validation through ingress filtering (Implement IETF BCP 38/RFC 2827) • Use Unicast Reverse Path Forwarding to mitigate problems that are caused by malformed or forged IP source addresses • Run separate DELEGATED and RESOLVING name servers • Disable Recursion on DNS server authoritative for the zone • Restrict zone transfers to slave name servers and other authorized software • Block invalid DNS messages to an authoritative name server at the network edge. This includes blocking large IP packets directed to an authoritative name server. • Check for version updates at the DNS server and install latest patches • Implement split DNS architecture • Implement anycast technology on DNS server
	Attacks on Servers, Routers, Firewall etc.	• Check for the effectiveness of filtering rules in the routers, firewall and IPS and reconfigure if required. • Replace compromised systems with trusted ones. • Check for version updates/patches and install latest

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

370

		patches for routers, firewall and IPS • Check the logs of these devices for source of attack
	Mail server attacks	• Activate hot standby mail servers and direct mail traffic appropriately.
	Advanced Targeted Attacks	• Identify the target entities and sensitize them about the targeted attacks • Isolate systems found to be connecting to suspicious domains/hosts after preserving volatile data and create forensic images for further analysis • Based on analysis of incident, apply appropriate security controls such as patching the targeted application, updating antivirus signatures to detect the crafted malware and detecting connections to call back domains/hosts through perimeter devices • Regularly monitor events and traffic at host/network level to detect malicious activities and report any suspicious activities to local IR team/CERT-In
	Attacks on Critical Infrastructure and associated SCADA/ Industrial Control Systems, through sophisticated malware such as Stuxnet/Duqu/Nitro	• Check for signs of infection in computer systems in general • Isolate infected systems from all networks immediately • Report the incident to local IR Team/CERT-In at the earliest. Consult relevant advisories of CERT-In and follow specific measures suggested therein • Take a forensic image and send to local IR Team/CERT-In • Clean the affected systems with the updated antivirus software. • Install updated Antivirus/anti-spyware on all systems (servers and Personal Computers) • Examine the vectors of propagation of worms – Removal media, network shares and other sneakernet systems. • Examine the critical SCADA/Industrial Control Systems/PLCs for abnormal functionality • Examine Critical systems of Industrial process for abnormal functionality • Examine network traffic towards malicious domains/websites/hosts that are indentified as Command & Control • Trace the infected PLCs/Systems and isolate immediately. • Review the security controls and processes to ensure isolation of critical networks from other infrastructure • Follow guidelines mentioned under Appendix VI in respect of dealing with air gap for isolation of control systems from other networks • Regularly track network connections and probing attempts in normal situations
	Compromise of trust infrastructure	In case of report of compromise or circulation of rogue

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

	- Certifying Authority, authentication mechanism, compromise of key management	certificate: • Immediately report the incident to concerned Ministry/Department and CERT-In • Revoke the compromised keys • Announce revocation notification at the earliest • Review the network/system security posture • Deploy appropriate mechanism to check and certify correctness of cryptographic functions • Generate fresh keys/certificates • Conduct appropriate awareness campaign to notify all users • Providers of App stores will need to pay special attention to implementation of trust and security functions in order to avoid serious impact on the user trust
		On report of the incident, CERT-In would take following supportive actions • Analyse and correlate the information/logs received from affected organisations • Check for latest patches/updates of system software, network devices and antivirus signatures from vendors and other sources • Consult the vendors and other sources to help the organisations in resolving the problems • Contact the concerned CERTs or ISPs from where the attacks are originating for blocking in case of DoS/DDoS attacks Document the resultant vulnerability, prepare vulnerability notes and disseminate to cyber community.
Level 3 Response **Scope:** **State/** **Multiple States**		**Responsibility:** **<mention Name of Respective Central Ministry/Department/State/UT >** • Notify the incidents to SCMC/NCMC, as the case may be • Depending up on the situation request for the meeting of SCMC/NCMC
		Steps to be taken by affected Organisations • Notify incidents to respective administrative

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

	All attacks	Ministry/Department • Implement the Contingency Plan • Deploy onsite response team on 24X7 basis • Limit the access to systems and networks from outside in consultation with concerned ISPs. • Enable hot stand-by systems/servers with alternate Traffic paths. • Take all logs (system, application, security, access, error etc) of affected systems and data therein and keep them separately for analysis and forensics • Segregate networks (LAN/WAN) and perimeter security devices and systems. Check for configuration vis-à-vis ongoing attack. Implement the appropriate eradication process and recovery of system files and data as prescribed against each attacks in level 1 & 2. • Carry out file integrity checks on all the systems • Restore systems from trusted back-ups and validate the systems and networks before connecting to Internet. • Change all user/root/administrator passwords in all systems and network devices
		Actions to be undertaken by CERT-In • Analyse the on-going attacks/traffic and seek assistance from Vendors and other CERTs if required • Work closely with affected organisations, ISPs and other agencies to provide all necessary help to mitigate the incident. • Advise appropriate measures to isolate systems/networks at organisations/regions.
Level 4 Response **Scope:** **Entire Nation**	All attacks	**Responsibility:** **<mention Name of Respective Central Ministry/Department/State/UT >** • Notify the incidents to SCMC • Request for the meeting of SCMC **Steps to be taken by affected Organisations** • Carry out all the steps indicated in level 3 • Implement directives of SCMC, respective administrative Ministry/Department • Implement specific advisories and instructions issued by CERT-In and other designated agencies.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

		Actions to be undertaken by CERT-In • Analyse the on-going attacks/traffic and seek assistance from Vendors and other CERTs if required • Work closely with affected organisations, ISPs and other agencies to provide all necessary help to mitigate the incident. • Advise appropriate measures to isolate systems/networks at organisations/regions.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Appendix – XIII Control Room Details of CERT-In & Incident Reporting Procedure

Primary Contact		
Name	**Designation**	**Contact Details**
Dr Sanjay Bahl	Director General	Tel Nos.
		Off: 011-24368544
		Res: 011-22323085
		Email: sanjay.bahl@nic.in
		Fax: 011-24366806

Alternate Contact		
Name	**Designation**	**Contact Details**
Sh. S.S Sarma	Operation Manager	Tel Nos.
		Off: 011-24368572 Ext: 209
		Email: sarma@cert-in.org.in
		Fax: 24301363

Incident Response Help Desk
Tel Nos: 1800-11-4949(Toll Free) Tel No: 011-24368572 Fax: 1800-11-6969 Email: incident@cert-in.org.in, info@cert-in.org.in

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Incident Reporting Procedures

Any organisation or corporate using computer systems and networks may be confronted with security breaches or computer security incidents.

By reporting such computer security incidents to CERT-In, the System Administrators and users will receive technical assistance in resolving these incidents. This will also help the CERT-In to correlate the incidents thus reported and analyze them; draw inferences; disseminate up-to-date information and develop effective security guidelines to prevent occurrence of the incidents in future.

2.1 Reporting of an incident

System Administrators can report an adverse activity or unwanted behaviour which they may feel as an incident to CERT-In. They may use the following channels to report the incident.

Email: incident@cert-in.org.in

Helpdesk +91-1800-11-4949 (Toll free)
Fax +91-1800-11-6969(Toll free)

2.2 Contents of Incident Report

The following information (as much as possible) may be given while reporting the incident.

- Time of occurrence of the incident
- Information regarding affected system/network
- Symptoms observed
- Relevant technical information such as security systems deployed, actions taken to mitigate the damage etc.

For details please refer the incident reporting form given in Para 2.6.

2.3 Verification

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

CERT-In will verify the authenticity of the report.

2.4 Triage

CERT-In will then analyse the information provided by the reporting authority and identify the existence of an incident. In case it is found that an incident has occurred, a tracking number will be assigned to the incident. Accordingly, the report will be acknowledged and the reporting authority will be informed of the assigned tracking number. CERT-In will designate a team as needed.

2.5 Incident Response

The designated team will assist the concerned System Administrator in following broad aspects of incident handling:

- Identification: to determine whether an incident has occurred, if so analyzing the nature of such incident, identification and protection of evidence and reporting of the same.
- Containment: to limit the scope of the incident quickly and minimise the damage
- Eradication: to remove the cause of the incident
- Recovery: taking steps to restore normal operation

CERT-In will provide support to the System Administrators in identification, containment, eradication, and recovery during the incident handling in the form of advice. CERT-In will not physically deploy or send any member for attending the incident response activity at the site of occurrence. The priority of assisting in responding to the incidents will be decided by CERT-In keeping in view the severity of incident and availability of resources.

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

377

Incident Reporting Form

Form to report Incidents to CERT-In			
For official use only: **xxxxxx**		Incident Tracking Number : **CERTIn-**	
1. Contact Information for this Incident:			
Name:	Organisation:	Title:	
Phone / Fax No:	Mobile:	Email:	
Address:			
2. Sector : (Please tick the appropriate choices)			
☐ Government ☐ Financial ☐ Power	☐ Transportation ☐ Manufacturing ☐ Health	☐ Telecommunications ☐ Academia ☐ Petroleum	☐ InfoTech ☐ Other _____
3. Physical Location of Affected Computer/ Network and name of ISP.			
4. Date and Time Incident Occurred:			
Date:	Time:		
5. Is the affected system/network critical to the organisation's mission? (Yes / No). Details.			

6. Information of Affected System:				
IP Address:	Computer/ Host Name:	Operating System (incl. Ver./ release No.)	Last Patched/ Updated	Hardware Vendor/ Model

7. Type of Incident:		
☐ Phishing ☐ Network scanning /Probing ☐ Break-in/Root Compromise ☐ Virus/Malicious Code ☐ Website Defacement ☐ System Misuse	☐ Spam ☐ Bot/Botnet ☐ Email Spoofing ☐ Denial of Service(DoS) ☐ Distributed Denial of Service(DDoS) ☐ User Account Compromise	☐ Website Intrusion ☐ Social Engineering ☐ Technical Vulnerability ☐ IP Spoofing ☐ Other_____

8. Description of Incident:

9. Unusual behavior/symptoms (Tick the symptoms)	
☐ System crashes ☐ New user accounts/ Accounting discrepancies ☐ Failed or successful social engineering attempts ☐ Unexplained, poor system performance ☐ Unaccounted for changes in the DNS tables,	☐ Anomalies ☐ Suspicious probes ☐ Suspicious browsing ☐ New files ☐ Changes in file lengths or dates ☐ Attempts to write to system

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

router rules, or firewall rules ☐ Unexplained elevation or use of privileges ☐ Operation of a program or sniffer device to capture network traffic; ☐ An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user ☐ A system alarm or similar indication from an intrusion detection tool ☐ Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server	☐ Data modification or deletion ☐ Denial of service ☐ Door knob rattling ☐ Unusual time of usage ☐ Unusual usage patterns ☐ Unusual log file entries ☐ Presence of new setuid or setgid files ☐ Changes in system directories and files ☐ Presence of cracking utilities ☐ Activity during non-working hours or holidays ☐ Other (Please specify)
10. Has this problem been experienced earlier? If yes, details.	
11. Agencies notified?	
☐ Law Enforcement	☐ Private Agency
☐ Affected Product Vendor	☐ Other_____
12. When and How was the incident detected:	
13. Additional Information: (Include any other details noticed, relevant to the Security Incident.)	
☐ Whether log being submitted	Mode of submission:
OPTIONAL INFORMATION	
14. IP Address of Apparent or Suspected Source:	

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Source IP address:	Other information available:

15. Security Infrastructure in place:				
	Name	OS	Version/Release	Last Patched/Updated
Name OS Version/Release Last Patched / Updated				
Anti-Virus				
Intrusion Detection/Prevention Systems				
Security Auditing Tools				
Secure Remote Access/Authorization Tools				
Access Control List				
Packet Filtering/Firewall				
Others				

16. How Many Host(s) are Affected		
☐ 1 to 10	☐ 10 to 100	☐ More than 100

17. Actions taken to mitigate the intrusion/attack:		
☐ No action taken ☐ System Binaries checked	☐ Log Files examined ☐ System(s) disconnected form network	☐ Restored with a good backup ☐ Other_____

Please fill all mandatory fields and try to provide optional details for early resolution of the Security Incident

Mail/Fax this Form to: CERT-In, Electronics Niketan, CGO Complex, New Delhi 110003 Fax:+91-11-24368546 or email at: incident@cert-in.org.in

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

Annexure-I

Control Room Details <*Indicate Contact détails of internal & external stakeholders Service providers*>

139

File No. T-21016/60/2023-eHealth (Computer No. 8225296)
Generated from eOffice by KAJAL GOEL, E-HEALTH-ASO(KG)-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 20/05/2024 02:03 PM

DDA AIIMS PATNA <dda@aiimspatna.org>

Model IT Infra plan for new AIIMS/ INIs-reg.

2 messages

VIKASH KUMAR GUPTA <vikas.kumar76@gov.in> Wed, May 28, 2025 at 12:09 PM
To: director <director@aiimsbhopal.edu.in>, director <director@aiimsbhubaneswar.edu.in>, director <director@aiimsjodhpur.edu.in>, director <director@aiimspatna.org>, director <director@aiimsraipur.edu.in>, director <director@aiimsrishikesh.edu.in>, director <director@aiimsmangalagiri.edu.in>, directoraiimsnagpur <directoraiimsnagpur@gmail.com>, drppjoshi <drppjoshi@aiimsnagpur.edu.in>, edaiimsrbl <edaiimsrbl@gmail.com>, rajwanshiarvind <rajwanshiarvind@hotmail.com>, ed <ed@aiimskalyani.edu.in>, executivedirector <executivedirector@aiimsgorakhpur.edu.in>, director <director@aiimsdeoghar.edu.in>, director <director@aiimsbibinagar.edu.in>, director <director@aiimsbilaspur.edu.in>, sharmadn <sharmadn@aiims.edu>, shakti810505 <shakti810505@gmail.com>, director <director@aiimsjammu.edu.in>, drmhraosvims1957 <drmhraosvims1957@gmail.com>, director <director@aiimsguwahati.ac.in>, madhabananda <madhabananda@gmail.com>, sachimohanty <sachimohanty@rediffmail.in>, dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, dda <dda@aiimsjodhpur.edu.in>, dda <dda@aiimspatna.org>, dda <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, rajeevsenroy30 <rajeevsenroy30@gmail.com>, dda <dda@aiimsbathinda.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, dda <dda@aiimsrbl.edu.in>, ddaaiimsrbl <ddaaiimsrbl@gmail.com>, kpradip10 <kpradip10@gmail.com>, dda <dda@aiimskalyani.edu.in>, dda <dda@aiimsgorakhpur.edu.in>, dda <dda@aiimsdeoghar.edu.in>, officeaiimsdeoghar <office.aiimsdeoghar@gmail.com>, ddaaiimsbibinagar <dda.aiimsbibinagar@gmail.com>, dda <dda@aiimsbibinagar.edu.in>, dda <dda@aiimsbilaspur.edu.in>, macprasad <mac.prasad@gmail.com>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, aps101982 <aps101982@rediffmail.com>, ddaaiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, aoaiimsmadurai <ao.aiimsmadurai@gmail.com>, tngamlien <t.ngamlien@icg.gov.in>, ddaaiimsawantipora1 <ddaaiimsawantipora1@gmail.com>, Arvind Thakur <arvind.thakur@nic.in>, Shalaka Kujur <shalaka.kujur@nic.in>, kumarakhilesh <kumar.akhilesh@gov.in>, ajay Kumar <ajay.kumar33@gov.in>, abhijitcgca <abhijit.cgca@gov.in>, praveenkumar67 <praveen.kumar67@nic.in>, ARUN BISWAS <ak.biswas57@nic.in>, Dharm Bir Kumar SIngh <dharmbk.singh@nic.in>
Cc: Shri Raj Kumar Deputy Secretary <raj.kumar28@nic.in>, RAHUL KUMAR SRIVASTAVA <rahul.srivastava@nic.in>, Ravi Kumar <ravi.kumar89@gov.in>

Sir/Ma'am

Please find attachment on the subject cited above for necessary action.

Thanks & Regards
Vikash Kumar Gupta, Central Secretariat Service (CSS)
Assistant Section Officer
PMSSY-I
Ministry of Health & Family Welfare
Govt. of India

Please consider your environmental responsibility. Before printing this e-mail message, ask yourself whether you really need a hard copy.

---

3 attachments

Letter-Model IT Infa plan for new AIIMSINIs-reg..pdf
83K

Model Cyber Security Plan for MoHFW Constitutents.pdf
4377K

National Cyber Security Policy - 2013.pdf
300K

Director . <director@aiimspatna.org> Wed, May 28, 2025 at 2:34 PM
To: DDA AIIMS PATNA <dda@aiimspatna.org>, Dr Abhyuday Kumar <drabhyudaykumar@aiimspatna.org>

Sd/-
Prof. (Dr.) Saurabh Varshney
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109
[Quoted text hidden]

---

3 attachments

Letter-Model IT Infa plan for new AIIMSINIs-reg..pdf
83K

Model Cyber Security Plan for MoHFW Constitutents.pdf
4377K

National Cyber Security Policy - 2013.pdf
300K

V-16020/67/2025-INI-I
Government of India
Ministry of Health and Family Welfare
PMSSY-I

Nirman Bhawan, New Delhi
Dated: 28-05-2025

To

Directors/Executive Directors
All new AIIMS

Subject: Model IT Infra plan for new AIIMS/ INIs-reg.

Sir/Ma'am

I am directed to refer to subject cited above and forward herewithModel Cyber Security Plan for AIIMS/INIs shared by CIRA (Copy enclosed) along with National Cyber Security Policy-2013 issued by MeitY (copy enclosed) for information and taking further necessary action.

2. This issues with the approval of the competent authority.

Encl: As above.

Yours faithfully

Digitally signed by Raj Kumar
Date: 28-05-2025 09:39:10

(Raj Kumar)
Deputy Secretary to GoI
Tele: 011-23063178

Copy to:
1. DDA, All new AIIMS
2.All Division Heads of PMSSY Division

Annexure D

Model Cyber Security Plan for MoHFW Constituents

1. Introduction:

All Hospitals/Medical Institutes deal with a lot of digitization owing to online booking, consultations and medical services & hence it is important to enhance the infrastructure's *Network Capacity and cyber security capabilities* , thus improving the *Security Posture* in the most effective and non-disruptive way possible.

Some of the guiding principles that these institutes need to align with in order to realize the aforementioned objective are:

- Best possible healthcare to patients visiting Hospital.
- Data safety of Personally Identifiable Information (PII) and Protected Health Information (PHI) of all patients visiting Hospital.
- Availability of online services such as Online Registration System (ORS), academic resources etc., as well as off-campus access to healthcare data.
- Efficient IT operations and security management.
- Enhanced network performance and scalability.

2. Best Practices:

Keeping up with cyber security threats has always been a challenge, but today the speed at which new threats are introduced is astounding. The sophistication of attacks and the use of advanced tools like artificial intelligence, machine learning, and other technologies are making ransomware, phishing, and other known forms of attacks more prevalent.

When it comes to security in healthcare, it's clear that uncertainty has become the new normal. Many organizations are not sure how to identify and manage digital risks in the ever-changing threat landscape, and their current risk management strategies just can't keep up. Cyber security breaches for healthcare organizations don't just have a negative impact on the financial and reputational standings of a healthcare organization. Breaches can involve the theft of protected health information (PHI) and personal identifiable information (PII), and can also result in longer patient stays, delays in procedures, and diversions to other facilities.

Medical device security is also a concern for healthcare providers, as bad actors take aim at vulnerable unpatched systems and improperly configured devices. We know that connected medical devices can represent a large percentage of the devices on a Healthcare Delivery Organization's (HDO) network. The proliferation of smart and connected medical devices will only continue as we see shifts in sites of care (from acute and post-acute sites to non-acute sites and home-based services).

1.4.1 Main Network

Main network should implement the 3-tier hierarchical wired and wireless LAN as per industry best practices to ensure resilient LAN infrastructure of Hospital.

File No. V-16020/12/2024-INI-I (Computer No. 8826194)
Generated from eOffice by MEESHI KUMAR-MUPTA ASO, UNDER SECRETARY, DEPARTMENT OF HEALTH & FAMILY WELFARE, DOHFW, DEPARTMENT on 28/05/2025 11:31 am

1.4.2 Guest WLAN

A physically separate Guest WLAN network should be established to provide internet access to guest users. The guests (Patients/Attendants) shall be provided access to internet through the captive portal. The captive portal shall provide temporary network access to guest users while maintaining security. This approach is particularly useful in organizations with a high volume of visitors. Guest WLAN components shall include (but not limited to):

1. Next generation Firewall
2. DNS, DHCP and IP address management services.
3. SMS based authentication
4. Captive portal based Wi-Fi internet access
5. Log server for keeping access logs

3. Architecture:

The design has two physically separate networks. First is Main network and second is Guest WLAN network.

1.5.1 Main Network

The main network provides connectivity to access CII and Non CII applications hosted in data centre, cloud hosted applications, limited & controlled Internet access, Wi-Fi Network access and other office functions for Hospital users.

The below Figure shows the Main Network Logical Topology.

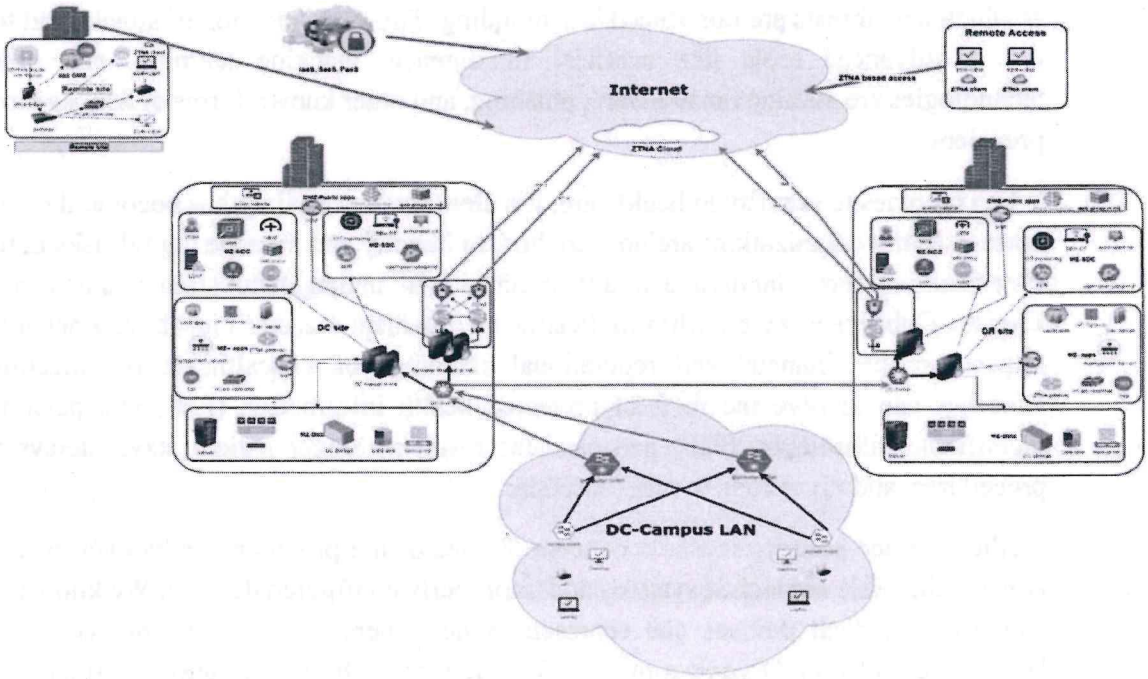


Figure 1: Main network logical Topology

* The main network Wi-Fi and guest WLAN Wi-Fi should be physically separate and non over lapping. Also, air-gap should be maintained between Operational network and Internet network.

File No. V-16020/82/2025/INI-I (Computer No. 8263946)
Generated from eOffice by NEELAM KUMAR GUPTA, ASO (UNDER SECRETARY TO THE DEPARTMENT) on 28/05/2025 11:31 am

1.5.2 Guest WLAN

The Guest WLAN caters to needs of Hospital Guest users i.e., Patients and attendants for internet services. Below Figure shows the Guest WLAN logical topology.

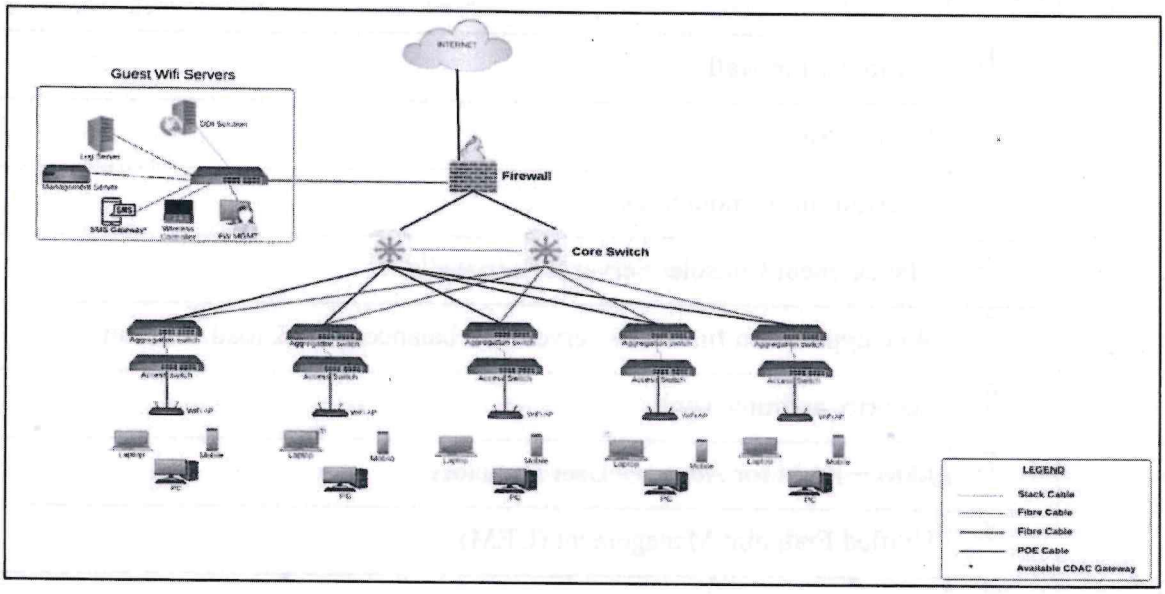


Figure 2: Guest WLAN Logical Topology

Necessary security measures have been proposed to ensure data security, redundancy, availability and backup. However as best practise it is recommended to review Hospital IT and Cyber security infrastructure periodically and update it as per latest security recommendations.

4. Cyber Security operations centre (SOC)

A security operations centre, or SOC, is a team of expert individuals and the facility in which they dedicate themselves entirely to high-quality IT security operations. A SOC seeks to prevent cyber security threats and detects and responds to any incident on the computers, servers and networks it oversees. What makes a SOC unique is the ability to monitor all systems on an on-going basis, as employees work in shifts, rotating and logging activity around the clock.

The SOC team stays ahead of potential threats by analysing active feeds, establishing rules, identifying exceptions, enhancing responses and keeping a close eye on possible vulnerabilities in the defences they have already set up. Ensuring these programs comply with company, industry and government regulations is also a significant part of a SOC's job.

Through their active surveillance and analysis, SOCs use strategic methodologies and processes to build and maintain the organization's cyber security defences.

File No. V-16020/02/2025-INH (Computer No. 8826346)
Generated from eOffice by VEELAM KUMAR-SUPT-MOHAN, UNDER SECRETARY, AND HOSPITAL DEPARTMENT on 28/05/2025 11:31 am

5. Components of the Design:

Sl. No.	Description
1.	Perimeter Firewall
2.	DC Firewall
3.	Firewall for Remote Sites
4.	Management Console/ Server for Firewalls
5.	Web application firewall + server load balancer +Link load balancer
6.	Security auditing Tool
7.	IAM + PAM for Admin + User Directory
8.	Unified Endpoint Management (UEM)
9.	Endpoint Detection and response (EDR)
10.	Network access control (NAC)
11.	Web Proxy
12.	NG-SIEM Solution including SOAR, UEBA and NDR
13.	DNS, DHCP and IP address management
14.	IT service management (ITSM)
15.	Network management system (NMS)
16.	Zero Trust Network Access for remote users
17.	Secure remote access

Guest WLAN:

Sl. No.	Description
1.	Firewall
2.	Log Server and S/W
3.	DNS, DHCP and IP address management
4.	Web proxy server
5.	WLAN Management including NAC (Network Admission Control)

File No. V-16020/02/2025-INHI (Computer No. [illegible])
Generated from eOffice by [illegible] on 28/05/2025 11:31 am

National Cyber Security Policy -2013

Preamble

1. Cyberspace[1] is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.

2. Owing to the numerous benefits brought about by technological advancements, the cyberspace today is a common pool used by citizens, businesses, critical information infrastructure, military and governments in a manner that makes it difficult to draw clear boundaries among these different groups. The cyberspace is expected to be more complex in the foreseeable future, with many fold increase in networks and devices connected to it.

3. Information Technology (IT) is one of the critical sectors that rides on and resides in cyberspace. It has emerged as one of the most significant growth catalysts for the Indian economy. In addition to fuelling India's economy, this sector is also positively influencing the lives of its people through direct and indirect contribution to the various socio-economic parameters such as employment, standard of living and diversity among others. The sector has played a significant role in transforming India's image to that of a global player in providing world-class technology solutions and IT business services. The government has been a key driver for increased adoption of IT-based products and IT enabled services in Public services (Government to citizen services, citizen identification, public distribution systems), Healthcare (telemedicine, remote consultation, mobile clinics), Education (e-Learning, virtual classrooms, etc) and Financial services (mobile banking / payment gateways), etc. Such initiatives have enabled increased IT adoption in the country through sectoral reforms and National programmes which have led to creation of large scale IT infrastructure with corporate / private participation.

4. In the light of the growth of IT sector in the country, ambitious plans for rapid social transformation & inclusive growth and India's prominent role in the IT global market, providing right kind of focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks, has become one of the compelling priorities for the country. Such a focus enables creation of a suitable cyber security eco-system in the country, in tune with globally networked environment.

[1] ISO / IEC 27032-2012

5. Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation- states and non-state actors. Cyber attacks that target the infrastructure or underlying economic well-being of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures. A cyber related incident of national significance may take any form; an organized cyber attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity. Some of the examples of cyber threats to individuals, businesses and government are identity theft, phishing, social engineering, hactivism, cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates, advanced persistent threats, denial of service, bot nets, supply chain attacks, data leakage, etc. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

6. There are various ongoing activities and programs of the Government to address the cyber security challenges which have significantly contributed to the creation of a platform that is now capable of supporting and sustaining the efforts in securing the cyber space. Due to the dynamic nature of cyberspace, there is now a need for these actions to be unified under a **National Cyber Security Policy**, with an integrated vision and a set of sustained & coordinated strategies for implementation.

7. The cyber security policy is an evolving task and it caters to the whole spectrum of ICT users and providers including home users and small, medium and large enterprises and Government & non-Government entities. It serves as an umbrella framework for defining and guiding the actions related to security of cyberspace. It also enables the individual sectors and organizations in designing appropriate cyber security policies to suit their needs. The policy provides an overview of what it takes to effectively protect information, information systems & networks and also gives an insight into the Government's approach and strategy for protection of cyber space in the country. It also outlines some pointers to enable collaborative working of all key players in public & private to safeguard country's information and information systems. This policy, therefore, aims to create a cyber security framework, which leads to specific actions and programmes to enhance the security posture of country's cyber space.

I. Vision

To build a secure and resilient cyberspace for citizens, businesses and Government

II. Mission

To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

III. Objectives

1) To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.

2) To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).

3) To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.

4) To enhance and create National and Sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.

5) To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources.

6) To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, pilot development, transition, diffusion and commercialisation leading to widespread deployment of secure ICT products / processes in general and specifically for addressing National Security requirements.

7) To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.

8) To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.

9) To provide fiscal benefits to businesses for adoption of standard security practices and processes.

10) To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cyber crime or data theft.

11) To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.

12) To create a culture of cyber security and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.

13) To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.

14) To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

IV. Strategies

A. Creating a secure cyber ecosystem

1) To designate a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities.

2) To encourage all organizations, private and public to designate a member of senior management, as Chief Information Security Officer (CISO), responsible for cyber security efforts and initiatives.

3) To encourage all organizations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices. Such policies should include establishing standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

4) To ensure that all organizations earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.

5) To provide fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security.

6) To prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cyber security compliance and proactive actions.

7) To establish a mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts.

8) To encourage entities to adopt guidelines for procurement of trustworthy ICT products and provide for procurement of indigenously manufactured ICT products that have security implications.

B. Creating an assurance framework

1) To promote adoption of global best practices in information security and compliance and thereby enhance cyber security posture.

2) To create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines (Eg. ISO 27001 ISMS certification, IS system audits, Penetration testing / Vulnerability assessment, application security testing, web security testing).

3) To enable implementation of global security best practices in formal risk assessment and risk management processes, business continuity management and cyber crisis management plan by all entities within Government and in critical sectors, to reduce the risk of disruption and improve the security posture.

4) To identify and classify information infrastructure facilities and assets at entity level with respect to risk perception for undertaking commensurate security protection measures.

5) To encourage secure application / software development processes based on global best practices.

6) To create conformity assessment framework for periodic verification of compliance to best practices, standards and guidelines on cyber security.

7) To encourage all entities to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and in networks.

C. Encouraging Open Standards

1) To encourage use of open standards to facilitate interoperability and data exchange among different products or services.

2) To promote a consortium of Government and private sector to enhance the availability of tested and certified IT products based on open standards.

D. Strengthening the Regulatory framework

1) To develop a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space (such as cloud computing, mobile computing, encrypted services and social media) and its harmonization with international frameworks including those related to Internet governance.

2) To mandate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to regulatory framework.

3) To enable, educate and facilitate awareness of the regulatory framework.

E. Creating mechanisms for security threat early warning, vulnerability management and response to security threats

1) To create National level systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

2) To operate a 24x7 National Level Computer Emergency Response Team (CERT-In) to function as a Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management. CERT-In will function as an umbrella organization in enabling creation and operationalization of sectoral CERTs as well as facilitating communication and coordination actions in dealing with cyber crisis situations.

3) To operationalise 24x7 sectoral CERTs for all coordination and communication actions within the respective sectors for effective incidence response & resolution and cyber crisis management.

4) To implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national processes or endangering public safety and security of the Nation, by way of well coordinated, multi disciplinary approach at the National, Sectoral as well as entity levels.

5) To conduct and facilitate regular cyber security drills & exercises at National, sectoral and entity levels to enable assessment of the security posture and level of emergency preparedness in resisting and dealing with cyber security incidents.

F. Securing E-Governance services

1) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan for all e-Governance initiatives in the country, to reduce the risk of disruption and improve the security posture.

2) To encourage wider usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.

3) To engage information security professionals / organisations to assist e-Governance initiatives and ensure conformance to security best practices.

G. Protection and resilience of Critical Information Infrastructure

1) To develop a plan for protection of Critical Information Infrastructure and its integration with business plan at the entity level and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

2) To Operate a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) to function as the nodal agency for critical information infrastructure protection in the country.

3) To facilitate identification, prioritisation, assessment, remediation and protection of critical infrastructure and key resources based on the plan for protection of critical information infrastructure.

4) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan by all critical sector entities, to reduce the risk of disruption and improve the security posture.

5) To encourage and mandate as appropriate, the use of validated and certified IT products.

6) To mandate security audit of critical information infrastructure on a periodic basis.

7) To mandate certification for all security roles right from CISO / CSO to those involved in operation of critical information infrastructure.

8) To mandate secure application / software development process (from design through retirement) based on global best practices.

H. Promotion of Research & Development in cyber security

1) To undertake Research & Development programs for addressing all aspects of development aimed at short term, medium term and long term goals. The Research & Development programs shall address all aspects including development of trustworthy systems, their testing, deployment and maintenance throughout the life cycle and include R&D on cutting edge security technologies.

2) To encourage Research & Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of cyber security challenges and target for export markets.

3) To facilitate transition, diffusion and commercialisation of the outputs of Research & Development into commercial products and services for use in public and private sectors.

4) To set up Centres of Excellence in areas of strategic importance for the point of security of cyber space.

5) To collaborate in joint Research & Development projects with industry and academia in frontline technologies and solution oriented research.

I. Reducing supply chain risks

1) To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices.

2) To build trusted relationships with product / system vendors and service providers for improving end-to-end supply chain security visibility.

3) To create awareness of the threats, vulnerabilities and consequences of breach of security among entities for managing supply chain risks related to IT (products, systems or services) procurement.

J. Human Resource Development

1) To foster education and training programs both in formal and informal sectors to support the Nation's cyber security needs and build capacity.

2) To establish cyber security training infrastructure across the country by way of public private partnership arrangements.

3) To establish cyber security concept labs for awareness and skill development in key areas.

4) To establish institutional mechanisms for capacity building for Law Enforcement Agencies.

K. Creating Cyber Security Awareness

1) To promote and launch a comprehensive national awareness program on security of cyberspace.

2) To sustain security literacy awareness and publicity campaign through electronic media to help citizens to be aware of the challenges of cyber security.

3) To conduct, support and enable cyber security workshops / seminars and certifications.

L. Developing effective Public Private Partnerships

1) To facilitate collaboration and cooperation among stakeholder entities including private sector, in the area of cyber security in general and protection of critical information infrastructure in particular for actions related to cyber threats, vulnerabilities, breaches, potential protective measures, and adoption of best practices.

2) To create models for collaborations and engagement with all relevant stakeholders.

3) To create a think tank for cyber security policy inputs, discussion and deliberations.

M. Information sharing and cooperation

1) To develop bilateral and multi-lateral relationships in the area of cyber security with other countries.

2) To enhance National and global cooperation among security agencies, CERTs, Defence agencies and forces, Law Enforcement Agencies and the judicial systems.

3) To create mechanisms for dialogue related to technical and operational aspects with industry in order to facilitate efforts in recovery and resilience of systems including critical information infrastructure.

N. Prioritized approach for implementation

To adopt a prioritized approach to implement the policy so as to address the most critical areas in the first instance.

V. Operationalisation of the Policy

This policy shall be operationalised by way of detailed guidelines and plans of action at various levels such as national, sectoral, state, ministry, department and enterprise, as may be appropriate, to address the challenging requirements of security of the cyberspace.

File No.:Z-28016/03/2024-PMSSY-V(8258126)
Government of India
Ministry of Health & Family Welfare
Department of Health & Family Welfare
(PMSSY-V Section)
****

Nirman Bhawan, New Delhi
Dated 17-06-2025

To

Executive Director,
All AIIMS under PMSSY.

Subject - Implementation of Swachhata Action Plan(SAP)-2025-26 - reg.

Sir/Madam,

I am directed to refer to the above mentioned subject and to forward herewith a copy of letter no. Z.28015/02/2023-H-II dated 03.06.2025 received from Hospital-II Section,MoHFW indicating the activities for which SAP funds are to be utilized.

In this regard, it is requested to take appropriate action and submit a quarterly progress report (physical and financial), to Under Secretary (Hospital-II), MoHFW.

Yours faithfully,
Digitally signed by
Dharm Bir Kumar Singh
Date: 17-06-2025
17:19:07
(Dharm Bir Kumar Singh)
Under Secretary to Govt. of India
Tele: 011-23060006

Copy to:

(i) Deputy Director Administration, All AIIMS under PMSSY.

No. Z.28015/02/2023-H-II (FTS: 8208289)
भारत सरकार / **Government of India**
स्वास्थ्य और परिवार कल्याण मंत्रालय / **Ministry of Health & Family Welfare**
स्वास्थ्य और परिवार कल्याण विभाग / **Department of Health & Family Welfare**
अस्पताल-II अनुभाग/ **Hospital-II Section**

Nirman Bhawan, New Delhi-110011
Dated 03-06-2025

To
As per attached list.

Sub: Provision of funds for implementation of Swachhata Action Plan (SAP) - 2025-26 in Central Government Hospitals/Institutes under Ministry of Health and Family Welfare-reg.

Madam/Sir,

I am directed to refer to the above mentioned subject and to say that the provision of funds has been made for implementation of SAP for the year 2025-26 in Central Government hospitals/ institutes. It is informed that funds allotted under SAP for the year 2025-26, is to be utilized on the Swachhta activities which is tabulated as under:-

Sl No.	Categories/ Activities	Programme/Activities (SAP Activities)
1.	Basic Maintenance	• Disposal of obsolete/un-serviceable items and equipment like electrical, electronic items, furniture, vehicles, waste papers etc. • Water sanitation and conservation practices, drainage and sewage, availability of adequate dustbins, maintenance of furniture and fixture. • Installation of Hepa filter, battery operated vehicles for transportation of patient within the hospital's campus • Swachhta Logo, Digital Signage,Water ATM, etc. • Maintenance and Inspection of Occupational, Functional Components and Structural Systems • Pest control services
2.	Sanitation and Hygiene	• Regular cleaning in wards, OT/OPD, Emergency, Lab/ICU/ICCU, toilet, workstations, disposable bins, door, walls, window. • Renovation of toilets for men and women and differently abled. • Regular review of such activities to be done on definite intervals. • Distribution of paper soap among the patient and attenders.

		• Installation of sanitary napkin vending machine and napkin incinerator
3.	Infection Control	• Handwashing, Personal protective equipment. • Use of gloves, face masks and head cap, apron/Lab coat during procedures and examination. • Decontamination and cleaning of instruments, environment control disinfection and sterilization of instruments. • Installation of automated hand sanitizers dispenser for all the wards/units, use of hand sanitizers and soaps • Procurement of fumigation machine and chemicals. • Infection control posters, IEC material etc.
4.	Cleaning and Beautification of surrounding areas	• Installation of herbal garden, beautification and landscaping, tree plantation, gardening. • Installation of potted plants in corridors to create an eco-friendly environment, etc. • Cleaning Office/hospital premises/Shramdan. • Plantation flower pants within the premises of hospital, cleaning of rainwater drainages.
5.	Digitization of Office records/e-office	• Digitization, storage and retrieval of Medical record, communications, files records, disposal of old file, implementation of e-office, • Online registration of patients, spare parts / software for digitization. • Queue Management System including token vending machine.
6.	Bio Medical Waste Management	• Disposal of bio-medical waste, collection Storage and transportation of biomedical waste. • Segregation practice of Bio-medical Waste as enumerated in Environment Act and Biomedical Waste Management Rules -2016, 2018 and 2019. • Solid and Liquid Waste Management • E-waste management • Management of hazardous waste, recycling of waste and statutory compliance. • Installation of waste-bins for segregate. • Chemical Waste Management
7.	Plastic Waste Management	• Prohibition of single-use plastic items such as PET bottles, plastic cups & plates, plastic jugs, plastic folders, plastic banner in the hospital and its surrounding areas, etc.

		• Collection and disposal of plastics waste, poster for "Not to use plastic". • Installation of shredder, plastic waste incinerator
8.	Hospital Safety	• Implementation of National Disaster Management guidelines for hospital safety • Awareness Generation for Hospital Safety • Safety of Hospital building. • Fire safety in hospital • Hospital disaster preparedness and response such as planning, training and drills, information, communication and documentation, Safety and Security etc. • Procurement of Mannequins for fire safety drills • Training, IEC Material, code-red posters workshop etc.
9	Hygiene promotion and Swachhta Awareness at Local level	• Competition like essay writing, slogan writing, painting etc. • Swachhta Awareness /Workshop • Display of banner/posters on Swachhata • Putting up of signages and captions like "No Smoking Area" "Do not Litter" etc. • Availability of information, education and communication (IEC) materials • Organize Swachhata pledge and various camps for promoting Swachhata in the community.

2. All the hospitals/ institutes are requested to take appropriate action and also submit its quarterly progress report (physical & financial) on timely basis to Hospital-II Section, Ministry of Health & Family Welfare.

Yours faithfully,

Digitally signed by
ANURADHA RAMAKRISHNAN
Date: 03-06-2025 11:53:48

(Anuradha Ramakrishnan)
Under Secretary to Government of India
Tele No. 2306 2319

Copy to:

(i) JS/EA concerned- for information & necessary action at their end.
(ii) US, PMSSY-V Section, MoHFW (with the request to intimate/ inform to all AIIMS under administrative control of PMSSY Division)

(iii) US, Hospital-I Section, MoHFW
(iv) US, H-III Section, MoHFW

Copy also to:-

The Joint Secretary (Shri Jitendra Srivastava), DDWS, M/o Jalshakti

List of Hospitals/Institutes

(1) Director, AIIMS, Ansari Nagar, New Delhi
(2) Director, AIIMS, Bhubaneswar
(3) Director, AIIMS, Bhopal
(4) Director, AIIMS, Jodhpur
(5) Director, AIIMS, Rishikesh
(6) Director, AIIMS, Patna
(7) Director, AIIMS, Raipur
(8) Director, AIIMS, Gorakhpur
(9) Director, AIIMS, Raebareli
(10) Director, AIIMS, Mangalagiri
(11) Director, AIIMS, Nagpur
(12) Director, AIIMS, Bathinda
(13) Director, AIIMS, Bibinagar
(14) Director, AIIMS, Kalyani
(15) Director, AIIMS, Deoghar
(16) Director, AIIMS, Bilaspur, Himachal Pradesh
(17) Director, AIIMS, Rajkot
(18) Director, AIIMS, Guwahati
(19) Director, AIIMS, Vijaypur (Jammu)
(20) Medical Superintendent, Dr. RML Hospital, New Delhi.
(21) Medical Superintendent, Safdarjung Hospital, New Delhi.
(22) Director LHMC and Associate Hospitals, New Delhi.
(23) Director, JIPMER, Dhanvantri Nagar, Gorimedu, Puducherry.
(24) Director, PGIMER, Karion Block, Sector-12, Chandigarh.
(25) Director, RIMS, Lamthelpat, Imphal, Manipur.
(26) Dean, Mahatma Gandhi Institute of Medical Sciences (MGIMS),Wardha
(27) Director, NEIGRIHMS, Shillong.
(28) Director, National Institute of Tuberculosis and Respiratory Diseases, New Delhi.
(29) Director, NIMHANS, Bengaluru
(30) Director, Central Institute of Psychiatry (CIP), Ranchi
(31) Director, Vallabhbhai Patal Chest Institute (VPCI), New Delhi
(32) Director, CNCI, Kolkata
(33) Director, RHTC, Najafgarh, New Delhi
(34) Director, Lokopriya Gopinath Bordoli Regional Institute of Mental Health (LGBRIMH), Tejpur, Assam
(35) Director, All India Institute of Speech and Hearing (AIISH), Mysore
(36) Director, All India Institute of Hygiene and Public Health, Kolkata

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Advisory Regarding Cyber Security Audit

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Wed, Dec 17, 2025 at 3:36 PM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **mn mishra** <mnmishra.mohfw@gmail.com>
Date: Mon, Jul 7, 2025 at 2:04 PM
Subject: Advisory Regarding Cyber Security Audit
To: <ciso@aiimskalyani.edu.in>, <anandchellappan@aiimsnagpur.edu.in>, <shivam.tsg@aiimsbhopal.edu.in>, <head.it@aiimsjammu.edu.in>, <rohit.bio@aiimsbibinagar.edu.in>, <drraje.path@aiimsmadurai.edu.in>, <drmohanraj@aiimsgorakhpur.edu.in>, <drabhyuday@aiimspatna.edu.in>, <raj.sharma@aiimsbhubaneswar.edu.in>, <Goyal.tarun@aiimsbathinda.edu.in>, <ciso@aiimsraipur.edu.in>, <draksharphc@gmail.com>, <itincharge@aiimsrishikesh.edu.in>, <aao@aiimsdeoghar.edu.in>, <mundraa@aiimsjodhpur.edu.in>, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, Deputy Director Administration <dda@aiimsbhubaneswar.edu.in>, <dda@aiimsdeoghar.edu.in>, DDA AIIMS Rishikesh <dda@aiimsrishikesh.edu.in>, DDA AIIMS Jodhpur <dda@aiimsjodhpur.edu.in>, DDA AIIMS Bhopal <dydir@aiimsbhopal.edu.in>, <ddamadurai1189@gmail.com>, DDA AIIMS PATNA <dda@aiimspatna.org>
Cc: RaviKumar RaviKumar <ravi.kumar89@gov.in>, ShriRajKumar Under Secretary <raj.kumar28@nic.in>, <arvind.thakur@nic.in>, <shalaka.kujur@nic.in>, <kumar.akhilesh@gov.in>, <abhijit.69@gov.in>, ANKITA MISHRA BUNDELA <js-pmssy-mohfw@gov.in>

Respected Sir/Madam,
This is to inform you that the Ministry has issued an advisory regarding timely completion of Security Audit .
In this regard, all AIIMS are requested to kindly take necessary action as per the details below:
Key Points:
Subject/Task: Security Audit of the institutional website/Software
Action Required: Conduct audit and share compliance certificate
Timeline: 10 July,2025
It is requested to ensure compliance with the above advisory and submit the Action Taken Report to this office by the stipulated date. Non-compliance may be viewed seriously at higher levels.
For any clarification, you may contact the undersigned.
Thank you for your cooperation.

With Regards,
Er.M.N.Mishra,
IT Consultant,
PMSSY,MoHFW,
Mob: 7982125857

11 attachments

Advisory No- TA-MAW-2025-06-26-022- QuasarRAT Malware [TLP- CLEAR].pdf
638K

Advisory No- TA-APT-2025-06-27-014- AresRAT (Linux Malware)- APT SideCopy Campaign [TLP-AMBER].pdf

405

591K

Advisory No- TA-APT-2025-06-25-013- APT BlueNoroff Recent Activity [TLP- CLEAR].pdf
607K

Advisory No- TA-MAW-2025-06-27-026- RemoteInjector Loader [TLP- CLEAR].pdf
653K

Advisory No- TA-PHI-2025-06-27-017- Phishing Attack [TLP- AMBER].pdf
623K

Advisory No- TA-MAW-2025-06-27-027- Malware Campaign Utilizing Commodity RATs [TLP- AMBER].pdf
361K

Advisory No- TA-MAW-2025-06-25-019- XDigo Malware [TLP- CLEAR].pdf
325K

Advisory No- VA-2025-06-24-018- Critical Vulnerabilities in Multiple Products [TLP- CLEAR].pdf
639K

Advisory No- TA-PHI-2025-06-24-014- Phishing Attack [TLP- AMBER].pdf
319K

Advisory No- TA-MAW-2025-06-25-017- SpyMax- Android Malware Campaign [TLP- AMBER].pdf
634K

Advisory No- TA-MAW-2025-06-25-018- ValleyRAT [TLP- CLEAR].pdf
604K

406

Fwd: Advisory No: TA-MAW-2025-06-26-022: QuasarRAT Malware [TLP: CLEAR]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Mon, 30 Jun 2025 11:04:04 AM +0530

To "reena.sharma80"<reena.sharma80@gov.in>,"Pawan Kumar" <pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@nic.in>

Mam/Sir

pl see for n/a

O/oJS(MKB)
23061066

========== Forwarded Message ==========
From : advisory@nciipc.gov.in
Date : Thu, 26 Jun 2025 15:07:08 +0530
Subject : Advisory No: TA-MAW-2025-06-26-022: QuasarRAT Malware [TLP: CLEAR]
========== Forwarded Message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-MAW-2025-06-26-022

Cyber Security Advisory: QuasarRAT Malware

This data is to be considered as TLP: CLEAR

Quasar is a lightweight and high-performance remote administration tool (RAT) for Windows, publicly available and developed in C# (C Sharp). It has been widely observed in various malware campaigns. Quasar RAT offers a range of capabilities, including screenshot capture, keylogging, system information gathering, remote shell access and command execution, reverse proxy functionality, task and file management, as well as the configuration and compilation of client executables.

Impacts:

- Data Theft and exfiltration : It can steal sensitive information, including personal data, financial records, and intellectual property, leading to potential identity theft or financial loss.
- System Compromise: The malware can gain unauthorized access to systems, allowing attackers to manipulate or damage files, disrupt operations, and compromise system integrity.
- Espionage: It can be used for spying on individuals or organizations, gathering confidential information, and conducting surveillance without the victim's knowledge.

Distribution Methods:

- Spread through spear phishing emails or exploitation of vulnerabilities in public-facing applications.

Tactics, Techniques, and Procedures (TTPs):

- Privilege Escalation-
  - T1053 (Scheduled Task/Job)
- Defense Evasion
  - T1562 (Impair Defenses)
  - T1140 (Deobfuscate/Decode Files or Information)
  - T1548 (Abuse Elevation Control Mechanism)
  - T1027 (Obfuscated Files or Information)
- Discovery
  - T1120 (Peripheral Device Discovery)
  - T1082 (System Information Discovery)
- Command and Control
  - T1071 (Application Layer Protocol)
  - T1105 (Ingress Tool Transfer)

**********IOC START**********

Domains:

connectdadad[.]ddns[.]net
yzs-42879[.]portmap[.]host
dez3452-33187[.]portmap[.]host
microsoftsys[.]ddns[.]net
letsqooo-62766[.]portmap[.]host
tpinauskas-54803[.]portmap[.]host

IP Addresses: Port

41[.]36[.]84[.]42:1339
137[.]184[.]144[.]245:4782
73[.]62[.]14[.]5:4782
182[.]253[.]58[.]75:4782
89[.]10[.]178[.]51:4782

**********IOC END**********

Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Enforce the use of Multi-Factor Authentication (MFA) across all remote access applications and services, including webmail and cloud-based email platforms.
- Apply MFA to critical accounts and infrastructure components, such as Domain Controllers, to further bolster their security.
- Establish and enforce a robust password policy across the organization.
- Implement a process for regular password resets enterprise-wide.
- Ensure that all devices within the organization are equipped with strong, up-to-date anti-malware and antivirus software.
- Configure your anti-malware and antivirus software to prevent access to websites and online resources that are known to distribute malicious links or attachments.
- Disable the Windows operating system's credential caching feature on devices where credentials are not necessary.

Reference: CERT-IN [CMTX-P062025826]
Note: TA-MAW: Threat Alert Malware Advisory

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: CLEAR. Recipients can spread this to the world, there is no limit on disclosure. Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

---

advisory@nciipc.gov.in mailing list





Fwd: Advisory No: TA-APT-2025-06-27-014: AresRAT (Linux Malware)- APT SideCopy Campaign [TLP: AMBER]

Madhukar Bhagat < jsehealth-mohfw@gov.in >

Mon, 30 Jun 2025 11:00:53 AM +0530

To "reena.sharma80"<reena.sharma80@gov.in>,"Pawan Kumar" <pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

pl see for n/a

O/oJS(MKB)
23061066

========== Forwarded Message ==========
From : advisory@nciipc.gov.in
Date : Fri, 27 Jun 2025 12:17:12 +0530
Subject : Advisory No: TA-APT-2025-06-27-014: AresRAT (Linux Malware)- APT SideCopy Campaign [TLP: AMBER]
========== Forwarded Message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-APT-2025-06-27-014

Cyber Security Advisory: AresRAT (Linux Malware)- APT SideCopy Campaign

This data is to be considered as TLP: AMBER

Linux-based malware is typically distributed in the Executable and Linkable Format (ELF) and is specifically designed to target Linux operating systems. ELF-based threats can vary in complexity, ranging from simple trojans and worms to advanced rootkits and ransomware. Such malware presents significant risks to servers, Internet of Things (IoT) devices, and other systems running Linux. Its objectives often include data exfiltration, botnet creation, and operational disruption.

Common Features Linux ELF Malware:

- Data Theft
- Remote Access
- Botnet Creation
- Persistence
- Rootkits
- Ransomware

**********IOC
START**********
IP:
185[.]235[.]137[.]237

**********IOC
END**********
Recommendations:

- It is recommended that organisations should apply the given IoC on their security systems to identify attacks. Occurrence of any communication traces pertaining to this IoC may be reported to NCIIPC.
- Be wary of unsolicited emails, especially those with attachments or links.
- Verify if the file extension matches the expected document type (e.g., .docx, .pdf, etc.). ELF executables typically have no extension or use unconventional extensions.
- Principle of least privilege.
- Firewall and network security along with regular OS updates.

Reference: CERT-IN [CMTX-I-792062025]
Note: TA-APT: Threat Alert - Advanced Persistent Threat Advisory

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: AMBER. Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Disclaimer:
The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

advisory@nciipc.gov.in mailing list





Fwd: Advisory No: TA-APT-2025-06-25-013: APT BlueNoroff Recent Activity [TLP: CLEAR]

Madhukar Bhagat < jsehealth-mohfw@gov.in >

Mon, 30 Jun 2025 11:06:01 AM +0530

To "reena.sharma80"<reena.sharma80@gov.in>,"Pawan Kumar" <pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@nic.in>

Mam/Sir

pl see for n/a

O/oJS(MKB)
23061066

========== Forwarded Message ==========
From : advisory@nciipc.gov.in
Date : Wed, 25 Jun 2025 17:20:14 +0530
Subject : Advisory No: TA-APT-2025-06-25-013: APT BlueNoroff Recent Activity [TLP: CLEAR]
========== Forwarded Message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-APT-2025-06-25-013

Cyber Security Advisory: APT BlueNoroff Recent Activity

This data is to be considered as TLP: CLEAR

A targeted cyberattack campaign has been observed, attributed to the BlueNoroff group also known by aliases such as TA444, Sapphire Sleet, COPERNICIUM, STARDUST CHOLLIMA, and CageyChameleon. This group operates under the broader umbrella of APT Lazarus/APT38. The campaign targets both macOS and Windows systems, using a Telegram-based social engineering lure. A malicious payload disguised as a Zoom browser extension was employed to deploy persistent implants, including backdoors, keyloggers, and cryptocurrency stealers. The attackers utilized advanced techniques, such as macOS process injection, to exfiltrate cryptocurrency-related data.

Potential Impacts:

- Full system compromise on macOS and Windows endpoints.
- Credential theft, data exfiltration, screenshot monitoring, covert long-term access.
- High risk to organizations working with Web3, crypto, fintech, and related sectors globally.

**********IOC
START**********

Domains:
productnews[.]online
firstfromsep[.]online
safefor[.]xyz
readysafe[.]xyz

URLs:
hxxps[://]safeupload[.]online
hxxps[://]metamask[.]awaitingfor[.]site/update
hxxps[://]support[.]us05web-zoom[.]biz/842799/check

Hashes:
4cd5df82e1d4f93361e71624730fbd1dd2f8ccaec7fc7cbdfa87497fb5cb438c
ad01beb19f5b8c7155ee5415781761d4c7d85a31bb90b618c3f5d9f737f2d320
ad21af758af28b7675c55e64bf5a9b3318f286e4963ff72470a311c2e18f42ff
432c720a9ada40785d77cd7e5798de8d43793f6da31c5e7b3b22ee0a451bb249
1ddef717bf82e61bf79b24570ab68bf899f420a62ebd4715c2ae0c036da5ce05
14e9bb6df4906691fc7754cf7906c3470a54475c663bd2514446afad41fa1527
469fd8a280e89a6edd0d704d0be4c7e0e0d8d753e314e9ce205d7006b573865f
080a52b99d997e1ac60bd096a626b4d7c9253f0c7b7c4fc8523c9d47a71122af
2e30c9e3f0324011eb983eef31d82a1ca2d47bbd13a6d32d9e11cb89392af23d

**********IOC
END**********

Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Immediately address known vulnerabilities and keep macOS, Windows, and Office fully updated.
- Limit or block PowerShell, VBS, and LNK file execution from untrusted sources using group policy or application control tools.
- Add malicious domains, IPs, and file hashes identified in the campaign to firewall, DNS, and endpoint blocklists.
- Educate users about social engineering via Telegram and fake software lures.
- Use EDR solutions to detect process injection, backdoors, and keyloggers. Hunt for anomalies in user behavior and system files.

Reference: CERT-IN [CMTX-P062025796]
Note: TA-APT: Threat Alert - Advanced Persistent Threat

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: CLEAR. Recipients can spread this to the world, there is no limit on disclosure. Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction.

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

advisory@nciipc.gov.in mailing list


2025
International Year
of Cooperatives
Cooperatives Build
a Better World
SANCHAR SAATHI
MOBILE APP
Web portal available at : www.sancharsaathi.gov.in

Fwd: Advisory No: TA-MAW-2025-06-27-026: RemoteInjector Loader [TLP: CLEAR]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Mon, 30 Jun 2025 11:00:10 AM +0530

To "reena.sharma80"<reena.sharma80@gov.in>,"Pawan Kumar" <pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

pl see for n/a

O/oJS(MKB)
23061066

========== Forwarded Message ==========
From : advisory@nciipc.gov.in
Date : Fri, 27 Jun 2025 15:25:04 +0530
Subject : Advisory No: TA-MAW-2025-06-27-026: RemoteInjector Loader [TLP: CLEAR]
========== Forwarded Message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-MAW-2025-06-27-026

Cyber Security Advisory: RemoteInjector Loader

This data is to be considered as TLP: CLEAR

It has been observed that RemoteInjector, a custom shellcode-based loader, is employed by an Advanced Persistent Threat (APT) group to deploy secondary payloads most notably Havoc and SystemBC directly into system memory via scheduled tasks. Designed for stealth and persistence, it integrates into legitimate operating system processes to evade detection by conventional security mechanisms.
RemoteInjector executes payloads entirely in memory, thereby circumventing traditional file-based detection methods. It leverages advanced evasion techniques, including Process Environment Block (PEB) walking, API resolution via stack strings, and process hollowing, to inject malware such as Remcos into legitimate processes, ensuring covert execution and sustained access to the compromised system.

Distribution Methods:

- Initial access: Achieved using stolen VPN credentials and exploitation of public-facing servers.
- Web shells: Dropped early in the campaign to maintain access.
- Loader deployment: RemoteInjector installed as part of scheduled tasks to invoke in-memory execution of payloads, avoiding disk footprints.

Impacts:

- Espionage: Used for credential harvesting, network reconnaissance, and establishing long-term presence.
- Lateral movement: Enabled via chaining tools (e.g., plink, Ngrok, ReverseSocks5) allowing access to IT and restricted OT (Operational technology) segments.
- Resilience: Facilitates re-entry post-containment via reactivation of dormant payloads, indicating high adversary intent and sophistication

TTPs (MITRE ATT&CK mapping):

- Initial Access:
  - Spearphishing Attachment (T1566.001)
- Execution:
  - PowerShell (T1059.001)
  - MSHTA (T1218.005)
- Persistence:
  - Registry Run Keys, Scheduled Tasks(T1547.001)
- Defense Evasion :
  - Process Hollowing, Obfuscated Scripts (T1055.012, T1027)
- Credential Access:
  - Credential Dumping (T1003)
  - Keylogging(T1056.001)
- Command & Control:
  - Encrypted Channel (TLS), Custom Protocols (T1071.001)
- Collection:
  - Screen Capture (T1113)
  - Audio Capture (T1123)

**********IOC START**********

Hashes:

E12E14EEAC7D8631C2EBE67F2192D16B
D28484F61FED7C74CD827FBFF5E19A10
BF6BA3F9FA93E2860A1041A443B318B7CD93A1D5
6bfca49597e5652b3f16d05b9a24dcf23e259e74
22BD09FBAB54963D4B0234585D33571A47A2DF569DBAB8B40988415AB0A3C37B
00218B08FB18D8AA987B1AD21AB5A3D6D32D4C82C485AA6FD2DE7A6A5B5741CF

**********IOC END**********

Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- MFA enforcement for VPN and privileged accounts.
- Patch critical services immediately (e.g., Biotime, IIS-Internet Information Services).
- Harden remote access: monitor/limit RDP and VPN.
- Eliminate unauthorized scheduled tasks; validate all existing tasks.
- Detect in-memory injection via EDR, focusing on process hollowing and suspicious parent-child behaviors.
- Deploy EDR/XDR with fileless activity visibility.
- Adopt zero-trust and micro-segmentation, isolating IT/OT environments.
- Enable behavioral analytics, alerting on unusual executable network use.
- Run regular threat hunting exercises targeting known TTPs and IOCs.

Reference: CERT-IN [CMTX-P062025995]
Note: TA-MAW: Threat Alert Malware Advisory

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: CLEAR. Recipients can spread this to the world, there is no limit on disclosure. Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

---

advisory@nciipc.gov.in mailing list





Fwd: Advisory No: TA-PHI-2025-06-27-017: Phishing Attack [TLP: AMBER]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Mon, 30 Jun 2025 10:58:05 AM +0530

To "reena.sharma80"<reena.sharma80@gov.in>,"Pawan Kumar" <pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

pl see for n/a

O/oJS(MKB)
23061066

========== Forwarded Message ==========
From : advisory@nciipc.gov.in
Date : Fri, 27 Jun 2025 17:30:24 +0530
Subject : Advisory No: TA-PHI-2025-06-27-017: Phishing Attack [TLP: AMBER]
========== Forwarded Message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-PHI-2025-06-27-017

Cyber Security Advisory: Phishing Attack

This data is to be considered as TLP: AMBER

It has been observed that government personnel have received phishing emails from spoofed/compromised email IDs and malicious domains. The email contains a password-protected archive file named "Operational Directions & Guidelines by CDS dated 17 jun25.zip", with the password provided within the body of the email. Upon extraction, the archive reveals a file titled "Operational Directions & Guidelines by CDS dated 17 jun25.ppam", which is an encrypted PowerPoint Add-in file. When the .ppam file is opened, it executes a VBA (Visual Basic for Applications) script that initiates a download of a file named "Cyber-Security-Advisory.pptx" from the following hyperlink "hxxps://govin.sorlastore[.]com/uploads/Cyber-Security-Advisory.pptx". This downloaded file is malicious in nature. In the background, the script also attempts to download and execute an additional file named "cyber.exe" from "hxxps://govin.sorlastore[.]com/uploads/cyber.exe". However, at the time of analysis, this executable file was non-functional. The associated IP address and domain are known to be malicious and currently active, posing a risk of credential compromise and further malware propagation.

Mitre ATT&CK Tactics and Techniques:

- TA0002: Execution

- T1059: Command and Scripting Interpreter
- TA0003: Persistence
  - T1543: Create or Modify System Process.
- TA0004: Privilege Escalation
  - T1543: Create or Modify System Process.
  - T1543.002: Systemd Service.
- TA0007: Discovery
  - T1518.001: Security software Discovery.
  - T1518: Software Discovery
- TA0005: Defense Evasion
  - T1027: Obfuscated File or Information
  - T1064: Scripting
  - T1070: Indicater the Removal
  - T1564.001: Hidden Files and Directories
- TA0011: Exfilteration
  - T1048: Exfiltration Over Alternative Protocol
- TA0011 : Command and Control
  - T1071: Application Layer Protocol.
  - T1071: Non-Application Layer Protocol.
  - T1071: Ingress Tool Transfer.

**********IOC
START**********

Filename:
Operational Directions & Guidelines by CDS dated 17 jun25.zip
Hashes:
07bd8e43da18ed27705822929336f134
70c6b5b42aab764381e1b24a441e203daa4f9860
f615ae5865e3b46a84a36c089dd19d7bceda0c4c9dd4e78102960717c1050cd7

Filename:
Operational Directions & Guidelines by CDS dated 17 jun25.ppam
Hashes:
3ae66b48d134347c3ff45957fce9fcf0
d63bd02f32f9cc2505d5b9bedef71520a59e0358
3640ba71b4e6498e24423f7f64b3ebb5eb44c11ceae2f3346d6a943c1aa362c9

**********IOC
END**********

Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Install and regularly update antivirus software.
- Install Updates and Patches regularly.
- Conduct regular backup practices and keep those backups offline or on a separate network.
- Implement Multi-Factor Authentication (MFA).
- Never click and execute email attachments from unknown sources.
- Never open links shared on social media from unknown sources.
- Never run unknown files with exaggerated titles.
- Users of nic.in and gov.in domains be sensitised about the threat vector.

Note: *TA-PHI: Threat Alert Phishing Advisory*

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067

Website: www.nciipc.gov.in

Toll Free: 1800-11-4430

This document is distributed as TLP: AMBER. Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

---

advisory@nciipc.gov.in mailing list





Fwd: Advisory No: TA-MAW-2025-06-27-027: Malware Campaign Utilizing Commodity RATs [TLP: AMBER]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Mon, 30 Jun 2025 10:57:21 AM +0530

To "reena.sharma80"<reena.sharma80@gov.in>,"Pawan Kumar" <pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

pl see for n/a

O/oJS(MKB)
23061066

========== Forwarded Message ==========
From : advisory@nciipc.gov.in
Date : Fri, 27 Jun 2025 17:46:58 +0530
Subject : Advisory No: TA-MAW-2025-06-27-027: Malware Campaign Utilizing Commodity RATs [TLP: AMBER]
========== Forwarded Message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-MAW-2025-06-27-027

Cyber Security Advisory: Malware Campaign Utilizing Commodity RATs

This data is to be considered as TLP: AMBER

An ongoing malware campaign leveraging commodity Remote Access Trojans (RATs) has been observed targeting a broad range of organizations. The campaign appears to be opportunistic and financially motivated, with no clear focus on any specific geography or industry sector. The infection vector primarily involves malicious emails containing lure documents in multiple languages. These emails deliver payloads through archive attachments or embedded links, ultimately leading to the deployment of RAT families such as Remcos and VenomRAT. These tools are commonly used by threat actors due to their general-purpose administrative, surveillance, and data exfiltration capabilities, and their source code is often publicly available or easily acquired through underground forums. Analysis indicates the use of shared or re-used command-and-control (C2) infrastructure, likely configured by individual threat actors rather than being part of a malware-as-a-service (MaaS) platform. Variability in payload delivery and infrastructure setup suggests non-standardized, independent deployment. The threat actors behind this campaign demonstrate low to moderate sophistication, relying heavily on publicly available malware, crypters, and loaders. Some components show incremental improvements in obfuscation and execution techniques, but the overall approach remains aligned with common “spray-and-pray” tactics—prioritizing rapid distribution over stealth or technical complexity. Although the campaign’s intensity has fluctuated,

associated indicators of compromise (IOCs) continue to appear intermittently, suggesting that some components remain active in the threat landscape.

MITRE ATT&CK Techniques:

- Initial Access
  - T1566 Phishing
- Execution
  - T1059.001 Command and Scripting Interpreter: PowerShell
  - T1059.005 Command and Scripting Interpreter: Visual Basic
  - T1059.007 Command and Scripting Interpreter: JavaScript
  - T1204.002 User Execution: Malicious File
  - T1559.001 Inter-Process Communication: Component Object Model
- Persistence
  - T1112 Modify Registry
  - TT1547.001 Boot or Login Autostart Execution: Startup Folder
- Privilege Escalation
  - T1055.001 Process Injection: Dynamic-link Library Injection
  - T1055.002 Process Injection: Portable Executable Injection
- Defense Evasion
  - T1027 Obfuscated Files or Information
  - T1070.004 Indicator Removal on Host: File Deletion
  - T1140 Deobfuscate/Decode Files or Information
  - T1562 Impair Defenses
  - T1620 Reflective Code Loading
- Discovery
  - T1082 System Information Discovery
- Collection
  - T1056.001 Keylogging
  - T1056.002 GUI Input Capture ;
  - T1113 Screen Capture
- Exfiltration
  - T1041 Exfiltration Over C2 Channel
- Impact
  - T1486 Data Encrypted for Impact
  - T1496 Resource Hijacking
  - T1499 Endpoint Denial of Service

**********IOC START**********

IPs:
51[.]222[.]121[.]200
102[.]165[.]46[.]145
191[.]252[.]153[.]239

Domains:
connected[.]gotdns[.]ch
comandoespecial2023[.]duckdns[.]org

URLs:
hxxp[:]//51[.]222[.]121[.]200/c.txt
hxxp[:]//51[.]222[.]121[.]200/rr.txt
hxxp[:]//51[.]222[.]121[.]200/v.txt
hxxp[:]//51[.]222[.]121[.]200/dllcliente.txt
hxxp[:]//51[.]222[.]121[.]200/renn.txt
hxxp[:]//102[.]165[.]46[.]145/run.txt
hxxps[:]//pastebin[.]com/raw/0FK5ax2D
hxxps[:]//pastebin[.]com/raw/iDWcsqbn
hxxps[:]//emailmarketing[.]locaweb[.]com[.]br/accounts/194373/messages/3/clicks/50055/8?envelope_id=3

hxxps[:]//emailmarketing[.]locaweb.com[.]br/accounts/188466/messages/16/clicks/74522/58?envelope_id=14
hxxps[:]//drive[.]usercontent[.]google[.]com/download?id=1q2SN6d6sfcOEexG19WaNLkwAtt4X_kCy&export=download
hxxps[:]//drive.google[.]com/uc?export=download&id=1TA1GpPntimJr_vhKOz8Wpm1vCpPCZ82Q
hxxps[:]//drive[.]usercontent[.]google[.]com/download?id=1TA1GpPntimJr_vhKOz8Wpm1vCpPCZ82Q&export=download
hxxps[:]//firebasestorage[.]googleapis[.]com/v0/b/rrrrrr-72f36.appspot.com/o/proyecto%2FNuevo%20documento%20de%20texto.txt?alt=media&token=07534c17-88df-44aa-843a-358f2783de10
hxxps[:]//firebasestorage[.]googleapis[.]com/v0/b/cobrabanguela-b0fb9.appspot.com/o/tecnicaroda.txt?alt=media&token=abb25612-4e6f-4acb-b7fc-e5d09cb16bd2
hxxps[:]//firebasestorage[.]googleapis[.]com/v0/b/rrrrrr-72f36.appspot.com/o/proyecto%2Fskype.txt?alt=media&token=d9d97dde-ba82-4237-8223-b6f9ce2dee88

VenomRAT Cluster Infrastructure URLs :
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/VNCExclude1.jpg
hxxps[:]//raw[.]githubusercontent[.]com/VenomBase64/Ngrok/master/DynamicST.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/DisableDefender1.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/DisableDefender2.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/DisableDefender3.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/EatingPinuts.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/FinalVCN.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/Hideme.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/Machete.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/RDPUpdate.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/VMprotectEncrypt.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/VNCExclude2.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/VNCInvisibleRootKit.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/adex.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/ff.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/hrdmin.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/myBulldog.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/myMemory.jpg
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/ngrok-stable-windows-amd64.zip
hxxps[:]//raw[.]githubusercontent[.]com/lisence-system/assemply/main/us.jpg
hxxps[:]//www[.]minpic[.]net/t/az94/1c03w4
hxxps[:]//www[.]minpic[.]net/t/bbpo/5nttj

Hashes:
00746e4ee7c427c2ccae6a383599453c834e5ea10eaaf842d878ebdac1ec3698
05d21fca97f6b1e286af8d1cbe22af1981af9cf387fe3cec7e2ca830f6447018
0b55d5ff1d371dbd13c7788066ab5f67ab78dc34df4bd14a42c43f8066c52138
0ee3383599a1c013553979f4cf8f7e2c84ae3b8ba8272f0ced8c4e2b456acdd0
116d1b4760bb356b4cc2b4c4da82371ac992a6b5f2a9257850ed7028cc85db67
1461c8880698496f61a100ea68d79dbb47f93428b1e7fc9aac901ff8bf400ba6
159163808b2bf4b5559fdda78faf7061a4205fe3db4ce0251be3fd4cdffaa797
1667ad0fc29fcd40ab17963a9ba023626b552faaec902e32cfc2b26a9880b0dd
1a11b3a80e7d51d6e3ebdd46d3d65e328fab2c55171ae0072cb31c3147cf76ad
1ab786491a84e3c5bce4ae6bcb301d81a665b00ec7169bce0e3befacc3562776
1b6f856b43a969108c5539994ce9fbb1aaf757caadf90c4d04dab1d9f7e3938d
29c6eeefb28778392662fb00c32f60b865a96b520f11c82d86b2c97d29b75f1b
2a5670019227fe42b858de1bc5800c89816f826e76b71eef7b63d4ca703eb025
2b7b107796956afd7d43960b31e7f203a992c4156e8fbd39ae15842920a99407
2bce067384481f98bb005c23ebda530881071e29a02c0252955352a207b8f77f
31c400430c28c2ca29976d862878eeb2c365ae4f4afc450eaa6459364cac143a
342cdec573452a0280dda91354b37cb724e0fbde6744b2ce5d0d6872b8e6bed8
34baa198824ab17a4a968b0bd062b7bc71c7166a71c14aa33e3672033c039a24
3661135802180398656 6a4bc2ade83c7d457a0fc8b775cd8514f1ffdf6da7375
3c9413d24af33723a54dee91ebea599a98a313f5bd8ba9c600c3749f5efba3af
3fc452863dc66976a6d40d91b9706053f1afa362e9c6f43d04fe4a4b526c148d
40334090129b697cbc3a15b8db274da49d1019c574f90c2cf160283eaeae3cc4
4265e2aeb5e03672cdc6f5a143ccba989099c2f087f7d12afd10ef3d10e7d642
45545982c60a0e05f95322e60d119c02579e4b0ef041ad525cb8248e3eb2053f
543930fcaedd5c67c2de42b99ef24ae18fa8c99b48b14483b6c7a9122215ff6d
5b4219b911b1b9a683b348c6de56d261f19018a3fab0f7742f81a6cb4a57f9bd
64827ca998c784e457d4897a5cc55d0bf52fc27d17ac91fc225c93a2352f82ee
6da884fdd905d0223a44f2a63ed5f85efbbe3d6c86ab8090b25f4da39137ed52

6de57f3b605336078c0343dfacdec4e9fc053588b9222d18c4c6348412f06b69
716b03ccd5735cac8700c4cf508290bb3abd099ccbec1eec07914cff19a541b0
7208ba234dcc8ca8b4cd69e38370d794b670efb6a927d21fa42b944267e23e25
77fa5b2bdb3dcae8e4d33158f67ac55315170d8b6dae1b0514b5266705a203ad
7d4d5c1f2697ceae00e64778811ea0b00d793cbb40e194e62d4d5e27cef1933a
7dd1336a533bc729ee9eec6a11b957cf1a2f398048f859d703fce9c7c10ec86a
814ae21ed3d41be8b3abd12d39ee8e0b2b284dbfb021317b884febad56ab4fa2
81b8863acc62252b30fc11d3c0434f36dde845bfcaca37c01957451eb0900083
85a2b742e068bbfc02ed0310628126685c1a06eb66c044c2fdb99e6d7a09f5ba
8de4861c4aca30b32685f9a1b78c307b6faa5011551ebf689babc7c42babb720
a2ef6e1f58a00b5d6523987df95a7ffc052a89470f97cd228a14fbccff113237
a6270d89a5d0a9a119e200f2f0cd669d5885f8a808f62e09f25cf94faa356ecd
b9bf9ed180d3838fb1f69eeb737cb5e6599bab680658673bcb1122487cf34bec
bc090c50e7dcd5dd77c64797bcf2c8544a7f2923043fc77be9c1b3d5a5e62266
bef0b231ac259d2e0f4b3d49201c915227d7818972cdc5030568ec9ac3cbb152
c2f960d6bce43b211090b4ab089cc9475f1762c78d1787b8f2c53800a2df0e2b
c9f81c638eaf4ccdc88cfff58a31a532b9816f8279e976e80d08766126db308e
ca6bea4917cf087196d9724bdfac9814f6e96f4e1b99b06adf3e03c7eadaa2a6
d2ae5e9ece390dee08e2aa6e56d8d084274d7d20a15523956896f7018d175308
d30740f5b84dafe7be3d2bded73dc98da16a6131f55940361087a3a7fb5b73cb
d694bcda645895f43eadf2d60e5d03e1a48b8fde5ecc77df5594ddf30f89dab1
d7899536f4692330536a76a973691eb78e2a8256350c119252afabbae88d78e1
d7fc49ea22ba4176919a7342ba7909ebfc5f76ec4031908bf3262f510030a8d9
d97916b289fe7681109dac830dbc58e171888894d4838424e75cc315f26ab522
dd35dd0eb6bb4526e505ef4431bfde4a592b6fb313a6b2ba1ff5b7a3c4921635
e02ed5061cdec08c9e33981f0d75819fc74caba852a830679e6e96e913ca8306
e3bf375ae95a318e4ea79c96e0e90a7fb8841371920f44c52260691691001c15
e50eab2b5a062ba0af3bec95fcf12637ac37e1d889c0cfbb6ae623d3bc25eb47
e9cc243923de94787673438f26c30baefe9995b38c8b8047b95726b998baf26c
ed6dd1b56c22e70a8f7ed2582803ce7731ab5d3210a065d26d34e2ac78e5ef6b
f5b6b9582eb2630439f2c58f0b81fcbff61b1069970d9e31df0cce6bfd5850c8
f5d110debc97e799257830a047b8045d3bc97d8c180753fd2b836507869d5226
f666ce7cd0fcb4bf2718c9fb6edcbd825bedae8fd57374931c82a7866975f37d
f771112a4c6d897a26b23d3d4e2e857ff24aad21e720dca0fa91f8a48c5bd3e9
fa9f51732139db3423f3c7e267203b2cd837c7cfe264a0bc4fd50d0c442ecd60
fe33c52f14bec607246474df8ef9391c000bc4082eb5ca5d6704edb2881f664f

**********IOC
END**********

Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Apply behavioral-based detection methods alongside traditional signature-based defenses.
- Strengthen email filtering and user awareness to mitigate phishing-based delivery methods.
- Regularly review and update endpoint and network-level threat detection rules.

Note: *TA-MAW: Threat Alert Malware Advisory*

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: AMBER. Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

advisory@nciipc.gov.in mailing list



Fwd: Advisory No: TA-MAW-2025-06-25-019: XDigo Malware [TLP: CLEAR]

Madhukar Bhagat < jsehealth-mohfw@gov.in >

Wed, 25 Jun 2025 5:02:59 PM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Wed, 25 Jun 2025 16:49:57 +0530
Subject: Advisory No: TA-MAW-2025-06-25-019: XDigo Malware [TLP: CLEAR]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-MAW-2025-06-25-019

Cyber Security Advisory: XDigo Malware

This data is to be considered as TLP: CLEAR

A Go-based malware variant known as XDigo has been identified and is reportedly being used in attacks targeting government entities. The infection chain involves a multi-stage delivery process, utilizing a sequence of Windows shortcut (LNK) files to deploy the malware. XDigo functions as an information-stealing tool, capable of collecting files, capturing clipboard contents, and taking screenshots. Additionally, it supports the execution of commands or binaries retrieved via HTTP GET requests, while exfiltrating stolen data through HTTP POST requests.

**********IOC START**********

Domains:
pdf-bazaar[.]com
pdfdepozit[.]com

file-bazar[.]com
vashazagruzka365[.]com
melodicprogress[.]com
pechalnoyebudushcheye[.]com
quan-miami[.]com
sogrevayushchiynapitok[.]com
seychaspozzhe[.]com
aoc-upravleniye[.]com
bukhgalter-x5group[.]com
bystryvelosiped[.]com
cellporyad[.]com
dversteklo[.]com
dwd765m[.]com
khoroshayamych[.]com
krasnayastena[.]com
magnitgroup[.]com
ru-pochta365[.]com
ru-sistema[.]com
temnayamashina[.]com
utrenneyesolntse[.]com
zelenyysalat[.]com
zhestovyyliker[.]com
zimniyeravlecheniya[.]com
laultrachunk[.]com
promenimath[.]com
slomannyymonitor[.]com
doverennyye-fayly[.]com
faylsklad[.]com
moy-pdf[.]com
nevynosimayapchela[.]com
pdf-reyestr[.]com
pdf-sklad[.]com
reyestr-faylov[.]com
serayagrust[.]com
protej.org.nniir[.]com
nniir[.]com
file-magazin[.]com
pdfmagazin[.]com
skachivanie-failov[.]com
chistyyvozdukh[.]com
svobodnoepredlozheniye[.]com
vash-disk[.]com
zagruzkadannykh[.]com
zetta-strakhovaniye[.]com
khitrayalisitsa[.]com
tvoi-fayly[.]com
kletchatayarubashka[.]com
downloading24[.]com
easy-download24[.]com
full-downloader[.]com
skachivanie-failov24[.]com
obmen-faylami[.]com
tvoy-disk[.]com
www[.]vashi-fayly[.]com
zagruzkafayla[.]com
faylbox365[.]com
zagruzka-pdf[.]com
moy-fayl[.]com
otpravkafaylov[.]com
pdfsklad[.]com

Hashes:
a28ee84bfbad9107ad39802e25c24ae0eaa00a870eca09039076a0360dcbd869
4f1d5081adf8ceed3c3daaaa3804e5a4ac2e964ec90590e716bc8b34953083e8
59b907430dde62fc7a0d1c33c38081b7dcf43777815d1abcf07e0c77f76f5894
ccf56b6b727da47c89f7a1a47cc04ab3a41d225c1298a74f16c939a5622b03f2
b03d9dd170cd82890ee1a5503529b81ce8064893e31a88b87081a8c72610d810
e14fdb6c0b5b64e1ca318b7ad3ac9a4fd6dec60ef03089b87199306eba6e0ca6
678f79e78847a1274238740bb8cada62f9c41cab96df8537d87d38850502d0a2

81bb1cf3a805c1375bb3251eea9f1ad132ab1266295a75cda9ffe9278588ac7f
d5c0fd26ba1504bde3222202f7a257efa9cdbc6949718495a7c33cd6510fce2a
52a98f2b2de46bc0835a11d2ba22b874a09788596507c13ac22b9b8877a8f3c6
bc0b9075e3b8504c4e0c7097c6be8aa05f96032053ec43e502d297136aaf375e
38489af1360af2cb7ba70f61e4c562fa63ce58e59576ba452db560f75ed1680a
dd279ea6c2a660ff7e70788af4a6c98524836c1b63beed756a77942c83de06fa
40bc204062a1f936c246fbffbed1a6bb41107ad9e5ad25df8970e4090258e145
564b2184a7f53d5f1680673ced354f5e956d897b7e1ea7d3f992cc38be6a9b20
7d6eb47ff307bebf87022575edd19181ad34ee5a5db1f408a25d16cd27d8aa2f
40e3fcfcc09fd84b2745b75e0e5e7beae866f4300ec8f36e2e9ab3197f198dcd
0b705938e0063e73e03645e0c7a00f7c8d8533f1912eab5bf9ad7bc44d2cf9c3
9c1acde0627da8b518b0522d6fed15cecf35b20ed8920628e9f580cfc3f450ed
5be9aba659baa089bcd253905deaf3f084f2b8f03701e90f2a46b36781165925
536cd589cd685806b4348b9efa06843a90decae9f4135d1b11d8e74c7911f37d
cfd0d56ca3d6c9ca232252570522c4b904be2807c461276979b1f8c551ccd4aa
904db68a915b4bbd0b4b2d665bb1e2c51fa1b71b9c44ce45ccd4b4664f2bfd8e
e62c3135fd708ee420cf767fa1654d8d66ff01f5160ddadf633e3cc5eaeaa926
65209053f042e428b64f79ea8f570528beaa537038aa3aa50a0db6846ba8d2ec
15277bfc6b784c373d535fbda9396bd16c15d990943423167602fb81b26d0f07
95060ba948948eea9bfc801731960b97d3efceb300622630afcbccfe12c21ccd
792c5a2628ec1be86e38b0a73a44c1a92475724535555e7996bb9d0a58e37b62b
5e34d754b0a938de7e512614f8fc6d7cd6c704f76b05044e07c97bd44bd5d591
68347b0c6494a56dd0f6492c6c56158b46bcaf44878a8741f6e63ff2946cf30f
7e04c69685d8612f7fc3512ad9ad1802a28428f75874b8717c0f04e939a3324d
f3f2c3c5836ce6e3cb92aa6dfc0f133e15a7fd169a3d1049b7d82e49d1577273
448245612a5388074e32251a0b44769170c586cc4c2ae06cd953c7a461ce34a6
747dfd7f0ca893034136fd286c737b55edc9276b5794a02c6dd3771da0342729
5248b0e4af1914762cc1c436a898d12d5f74980b816155f4191dc9692402668f
7a2af22372a4fd3ba89d36fdee38967cb77f43e14255d0b5ad80da863b146625
7c0597aa77031a100db0941921b60f08079bec7f710b6e736a15012db6465c39
031e05d15afabef6010179d2acd09925395167fd442b64b6aa8ffd81bd5e268e
056cd36bf4bc6efc119a64f2ffedd76f3dcb75daa95c22c59d91664dfcaa6fd5
fb1df37336d79861b13d5f4ba875393c7e91b12cd73302cb414c1d084104a6a8
c8899a6e8d3dd11c75217253f8dd78f5029c01e886880cafce0388d5fd6aa54b
7a2af22372a4fd3ba89d36fdee38967cb77f43e14255d0b5ad80da863b146625
0d983f5fb403b500ec48f13a951548d5a10572fde207cf3f976b9daefb660f7e
3adeda2a154dcf017ffed634fba593f80df496eb2be4bee0940767c8631be7c1
49714e2a0eb4d16882654fd60304e6fa8bfcf9dbd9cd272df4e003f68c865341
e32f04362ec4db90e024bfb57adf6e5c02f1061cd17dbf81a5bbc0b588119b25
ffc538f2c6e91f07be067311ed143d28c5437a8af69974f751c043e2944d60b2
efd44bc4e0efcab72106ea065c8a89d51d499202732319b21324487e8d00eccf
2dde92fc0936cb275be79d5864c98772d1270e4a54c01e61ebc4b856b5e048d5
666f4977abf17db6da2d05b385c5cf53f6500517226a3ac5bd0360eda9193d08
be6a545180300554eea2ee6ece9f835a12996059d726df810fe13ba0044033cd
07e2376d2c4318b0f9c472d01342d67e23a2e8edc182533a291336dfeaff4e60
12fd8d45a181adfd6725ea9806d72ed61b3af1e31d80fa7ddd32e1932a8dfd75
bcb5df098a79e3bc1d8bcb3b1a354b6643afdb4ca40333e0548e5ed1a9470cac
f7be89ae645831d519b7c781d69cf8e88e5762b824c9a6753eb16b25c4abef76
a8d578d4b50ac4029db22b76563e927ab691075aacc87621795b16b388b7d48c
ef8fdec66751b6a17da45dd4d9c22cef8d3c78604e7a8bc6fc8e2b30342ff408
9f17ff59172a802bc6ce8490c1ea379a5bf75af839f8b59373fba8c51e878af0
0993b0bb897402954eb9057bc84ea98e2c12ff1185a87ac3c3a15a241560bb1a
0a626f1837da9043e65ccf9e23192aef36d58402a1fd56577952c7bb426f2ec5
e0ffc3442215b888c55d8dfd9d33c5cfff315a59089aeb42da4cf6869eed8f5d
77b2f2ef5bc3b7bb2d1b85491ece85b56da37685652526c6fa6e3562cd12e3b6
021d13de99e996fbf03e57b78ce67630c19d33242eee8480383d7b065edebb51
83341b08425a1a247becd79e829064ddbd309636d7d62a369338ffd47af6e955
5409eb70942a6b875d8343437bb04e368f56de1854953fa87890fc8ee8a8bc37
a9b9022aedd1b9afbd7ab1f11f60f236102e1f70b340658da8cb39c072a9af61
155b94be1c3dca48314f6f2ee0c89c09553851ecc9ceefc436e16ebb7fca5f1a
2414dd462e3ca05ecd37aa56dc8841f5ef9588663572e7bc36d07520af7864b1
bbc5e80d3f068d8eff0cfa745ecba97903a83dfd9fe6f43cf05e803bbe9ce8b9
e95f2982195399b5f9e453be6db02a346bb516320659a3ade2c385bcb7fc27da
ef34c433c818774b466ba4e6f677b1c6cf51bb9213a60fd779fd7df39011e97b

**********IOC
END**********

Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Train users to avoid opening suspicious .LNK files or attachments from unknown sources.
- Use EDR solutions to detect and block behaviors like clipboard access or unauthorized screenshot capture.
- Configure email systems to block or scan LNK files before delivery to users.
- Monitor for unusual HTTP GET/POST traffic, especially to unknown domains.
- Keep offline backups and verify they can be restored when needed.

Reference: CERT-IN [CMTX-P062025816]
Note: *TA-MAW: Threat Alert Malware Advisory*

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: CLEAR. Recipients can spread this to the world, there is no limit on disclosure. Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction.

Disclaimer:
The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

advisory@nciipc.gov.in mailing list



Fwd: Advisory No: VA-2025-06-24-018: Critical Vulnerabilities in Multiple Products [TLP: CLEAR]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Wed, 25 Jun 2025 4:08:52 PM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Tue, 24 Jun 2025 17:04:41 +0530
Subject: Advisory No: VA-2025-06-24-018: Critical Vulnerabilities in Multiple Products [TLP: CLEAR]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: VA-2025-06-24-018

Cyber Security Advisory: Critical Vulnerabilities in Multiple Products

This data is to be considered as TLP: CLEAR

Exposure of Sensitive Information vulnerability in Sapido Wireless Router
Multiple wireless router models from Sapido are affected by exposure of sensitive information vulnerability allowing unauthenticated remote attackers to directly access a system configuration file and obtain plaintext administrator credentials. Affected models are BR071n, BR261c, BR270n, BR476n, BRC70n, BRC70x, BRC76n, BRD70n, BRE70n, BRE71n, BRF61c, BRF71n. The affected models are out of support. It is recommended to replace the devices.
CVE ID: CVE-2025-6560 (Critical)
Reference: https://nvd.nist.gov/vuln/detail/CVE-2025-6560

OS Command Injection vulnerability in Sapido Wireless Router

Multiple wireless router models from Sapido are affected by OS Command Injection vulnerability allowing unauthenticated remote attackers to inject arbitrary OS commands and execute them on the server. Affected models are BR071n, BR261c, BR270n, BR476n, BRC70n, BRC70x, BRC76n, BRD70n, BRE70n, BRE71n, BRF61c, BRF71n. The affected models are out of support. It is recommended to replace the devices.
CVE ID: CVE-2025-6559 (Critical)
Reference: https://nvd.nist.gov/vuln/detail/CVE-2025-6559

Multiple vulnerabilities in ELECOM wireless LAN routers
Multiple vulnerabilities have been identified in ELCOM wireless LAN routers. An attacker can exploit these vulnerabilities to take control of an affected system.
CVE ID: CVE-2025-48890 (Critical), CVE-2025-43879 (Critical), CVE-2025-43877 (Medium), CVE-2025-41427 (High), CVE-2025-36519 (Medium)
Reference: https://jvn.jp/en/jp/JVN39435597/index.html

Vulnerability NetScaler ADC and NetScaler Gateway
A vulnerability has been discovered in NetScaler ADC and NetScaler Gateway. Affected versions are:
NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-43.56,
NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-58.32,
NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.235-FIPS and NDcPP and
NetScaler ADC 12.1-FIPS BEFORE 12.1-55.328-FIPS.
An attacker can exploit these vulnerabilities to take control of an affected system.
CVE ID: CVE-2025-5777 (Critical), CVE-2025-5349 (High)
Reference: https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420

Note: *VA: Vulnerability Advisory*

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: CLEAR. Recipients can spread this to the world, there is no limit on disclosure. Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction.
Disclaimer:
The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems

advisory@nciipc.gov.in mailing list





Fwd: Advisory No: TA-PHI-2025-06-24-014: Phishing Attack [TLP: AMBER]

Madhukar Bhagat < jsehealth-mohfw@gov.in >

Wed, 25 Jun 2025 4:08:12 PM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Tue, 24 Jun 2025 17:41:18 +0530
Subject: Advisory No: TA-PHI-2025-06-24-014: Phishing Attack [TLP: AMBER]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-PHI-2025-06-24-014

Cyber Security Advisory: Phishing Attack

This data is to be considered as TLP: AMBER

It has been observed that government personnel have received phishing emails from spoofed/compromised email IDs and malicious domains. The email contains an archive file named "Force Structure Devp 16 jun 25.zip", which is password-protected. The password is provided within the body of the email. Upon extraction, the archive reveals a file titled "Force Structure Devp 16 jun 25.ppam". This file is a PowerPoint Add-in file embedded with VBA macros and is identified as malicious. When the file "Force Structure Devp 16 jun 25.ppam" is opened, it contains a hyperlink "hxxps://govin.sorlastore[.]com/uploads/myprogram.exe". On clicking the hyperlink, it initiates the download of an executable file named "myprogram.exe", which is confirmed to be malicious and targets Windows operating systems.

Upon execution, "myprogram.exe" establishes a network connection with the domain "modgovin[.]onthewifi[.]com". The behavior of this file is flagged by multiple detection indicators,

including: detect-debug-environment, long sleep, macro-powershell, and obfuscated. The file performs following functions:-

- Execution
- File System
- Defense Evasion
- Discovery
- Persistence
- Anti behavioral Analysis

The IP address and domain involved are malicious and currently active, potentially compromising the user credentials/propagating malware payload.

Mitre ATT&CK Tactics and Techniques:

- TA0002: Execution
  - T1106: Windows Management Instrumentation
  - T1159: Command and Scripting Interpreter
  - T1129: Shared Modules
  - T1106: Native API
  - T1159.001: Power Shell
- TA0003: Persistence
  - T1574.002: DLL side Loading
  - T1542: Pre-OS Boot
  - T1574.003: Window Service
- TA0004: Privilege Escalation
  - T1574.002: DLL side Loading
  - T1574: Hijack Execution Flow
  - T1055: Process Injection
- TA0006: Credentials Access
  - T1539: Steal Web Session cookies
- TA0007: Discovery
  - T1083: Application Window Discovery
  - T1497: Virtualization/Sandbox Evasion
  - T1057: Software Discovery
  - T1016: System Network Configuration Discovery
- TA0011 : Command and Control
  - T1071: Application Layer Protocol.
  - T1095: Non Application Layer Protocol.
  - T1573: Encrypted Channel.
  - T1571: Non-Standard Port.
- TA0005: Defense Evasion
  - T1064: Scripting
  - T1014: Rootkit
  - T1027: Obfuscated Files or Information
  - T1027.001: Software Packing
  - T1036: Masquerading
  - T1055: Process Injection
  - T1202: Indirect Command Execution
  - T1497: Virtualization/Sandbox Evasion
  - T1202: Indirect Command Execution
  - T1562.001:Disable or Modify Tools
  - T1070.004: File Deletion
  - T1564: Hide Artifacts
  - T1574.002: DLL side Loading
  - T1542: Pre-OS Boot

**********IOC START**********

IPs:

158[.]247[.]7[.]206
101[.]99[.]92[.]182

433

Domain:
modgovin[.]onthewifi[.]com

Filename:
Force Structure Devp 16 jun 25.zip
Hashes:
87dafa8ba4f6940664d645cf017ffbcf
e373a5039ba8a9bb2c2126b1eff3e50e15b0e737
7a13fa30978f4a73d0af1799fd2010e251420e2618cb543cd35b1fb493cef238

Filename:
Force Structure Devp 16 jun 25.ppam
Hashes:
41bb66ae50f6a736fd91cb0d9892725d
d988026992dfb0a50a875eccacd3ccd189006072
de921d2906be8c371a08fcf03cb4de5d9663c1ec80f2097384e4e8943a1b757e

Filename:
Myprogram.exe
Hashes:
33e1da22fb1068c73c033e3bc6bd3f1e
7dea0506cff8f5d2d0c60a780c855da5df20a013
167b387005d6d2a55ad282273c58d1786a2ee0fa3e7e0cb361d4d61d8618ee5f

**********IOC
END**********

Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Install and regularly update antivirus software.
- Install Updates and Patches regularly.
- Conduct regular backup practices and keep those backups offline or on a separate network.
- Implement Multi-Factor Authentication (MFA).
- Never click and execute email attachments from unknown sources.
- Never open links shared on social media from unknown sources.
- Never run unknown files with exaggerated titles.
- Users of nic.in and gov.in domains be sensitised about the threat vector.

Note: *TA-PHI: Threat Alert Phishing Advisory*

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: AMBER. Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

---

advisory@nciipc.gov.in mailing list



Fwd: Advisory No: TA-MAW-2025-06-25-017: SpyMax- Android Malware Campaign [TLP: AMBER]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Wed, 25 Jun 2025 4:05:42 PM +0530

To "reenasharma80"<reena.sharma80@gov.in>
Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Wed, 25 Jun 2025 12:27:11 +0530
Subject: Advisory No: TA-MAW-2025-06-25-017: SpyMax- Android Malware Campaign [TLP: AMBER]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-MAW-2025-06-25-017

Cyber Security Advisory: SpyMax- Android Malware Campaign

This data is to be considered as TLP: AMBER

It has been observed that "SpyMax" is a mobile-based Remote Access Trojan (RAT) primarily targeting Android platforms. The malware is engineered to gain unauthorized access to infected devices, exfiltrate sensitive information, and conduct surveillance on victims. SpyMax is typically distributed through malicious applications, counterfeit software updates, or trojanized APKs that impersonate legitimate software to deceive users. Upon installation, it leverages elevated device permissions to conduct a range of malicious activities, including credential theft, call recording, screen capturing, camera activation, and unauthorized access to SMS messages and contact data. Furthermore, the malware establishes persistent communication with a Command-and-Control (C2)

server, enabling remote attackers to issue commands and maintain ongoing control over compromised devices.

Distribution Method:

- Phishing campaigns via messaging apps: lure users into clicking “Download” on fake app pages, triggering the download of ready.apk.
- Deceptive visuals: mimic familiar app logos and fake accessibility settings screens to build user trust.

Impacts:

- Keystroke logging: records typed credentials and messages in log files stored locally.
- Location tracking: captures latitude, longitude, speed, altitude .
- Data exfiltration: compresses and sends sensitive data to C2; receives APK payloads and commands in return .
- Complete device control: potential for surveillance, credential theft, fraudulent transactions, OTP interception, even camera/microphone abuse.

Tactics, Techniques, and Procedures (TTPs):

- Initial Access: Delivered through phishing campaigns or third-party app stores hosting malicious APKs.
- Execution: Exploits Android device permissions to execute surveillance operations. Can send SMS messages, intercept two-factor authentication codes, or manipulate device settings.
- Persistence: Operates in stealth mode, hiding its icon and running in the background to avoid detection.
- Exfiltration: Steals data (e.g., text messages, call logs, credentials) and sends it to the attacker's C2 server. Enables real-time spying via the device's microphone or camera.

**********IOC START**********

Hashes:
c58b2bacd7c34ef998497032448e3095
66a7fd9bd39b1ba0c097698b68fd94a7

IP:
104[.]234[.]167[.]145

**********IOC END**********

Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Install apps only from official stores. Avoid downloading apps from untrusted or unofficial sources.
- Grant apps only the minimum required permissions.
- Deploy mobile security solutions to detect and block malware.
- Keep Android devices and apps up to date with the latest security patches.
- Use Android's "Google Play Protect" and enable app verification.
- Never enable “Install from unknown sources” for persistent installs; disable after use.
- Scrutinize permissions—deny Accessibility access to unverified apps.
- Be vigilant of unsolicited “wedding invite” or “update” APK links shared via messaging apps.
- Deploy mobile threat defense with behavioral and network anomaly detection.
- Monitor network traffic to detect communications with suspicious IPs
- Encourage MFA and segregate work vs personal device use where possible.
- Train users to recognize phishing attempts and suspicious application behavior.

References: CERT-IN [CMTX-P062025115] & [CMTX-I-785062025]
Note: *TA-MAW: Threat Alert Malware Advisory*

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: AMBER. Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Disclaimer:
The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

---

advisory@nciipc.gov.in mailing list





Fwd: Advisory No: TA-MAW-2025-06-25-018: ValleyRAT [TLP: CLEAR]

Madhukar Bhagat < jsehealth-mohfw@gov.in >

Wed, 25 Jun 2025 4:05:11 PM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Wed, 25 Jun 2025 15:54:42 +0530
Subject: Advisory No: TA-MAW-2025-06-25-018: ValleyRAT [TLP: CLEAR]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-MAW-2025-06-25-018

Cyber Security Advisory: ValleyRAT

This data is to be considered as TLP: CLEAR

ValleyRAT is a sophisticated Remote Access Trojan (RAT) attributed to threat actors who deliver it through phishing campaigns and malicious downloads. ValleyRAT features a highly modular architecture and incorporates multiple layers of obfuscation along with custom encryption mechanisms, significantly complicating detection and analysis. The malware leverages a variety of advanced techniques, including process injection, registry manipulation, and User Account Control (UAC) bypass, to maintain persistence and evade security measures.

**********IOC START**********

IP Addresses: Ports

202[.]79[.]172[.]16:6666
46[.]8[.]122[.]64:1555,2555

193[.]112[.]101[.]108:6908

**********IOC
END**********

Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Deploy advanced email filtering solutions to detect and block phishing emails.
- Conduct regular training sessions to educate employees about phishing tactics and safe email practices.
- Utilize endpoint detection and response (EDR) tools to identify and respond to suspicious activities.
- Regularly update and patch systems to close vulnerabilities that could be exploited by malware.
- Implement network segmentation to limit the spread of malware within the organization.

Reference: CERT-IN [CMTX-P062025806]
Note: *TA-MAW: Threat Alert Malware Advisory*

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: CLEAR. Recipients can spread this to the world, there is no limit on disclosure. Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction.

Disclaimer:
The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

advisory@nciipc.gov.in mailing list





Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Cyber Security Advisory received From the National Critical Information Infrastructure Protection Centre (NCIIPC) reg.

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Wed, Dec 17, 2025 at 3:35 PM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **mn mishra** <mnmishra.mohfw@gmail.com>
Date: Fri, Jul 11, 2025 at 2:08 PM
Subject: Fwd: Cyber Security Advisory received From the National Critical Information Infrastructure Protection Centre (NCIIPC) reg.
To: <dda@aiimsdeoghar.edu.in>, DDA AIIMS Jodhpur <dda@aiimsjodhpur.edu.in>, DDA AIIMS Bhopal <dydir@aiimsbhopal.edu.in>, <ddamadurai1189@gmail.com>, Deputy Director Administration <dda@aiimsbhubaneswar.edu.in>, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Rishikesh <dda@aiimsrishikesh.edu.in>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, <ddaaiimsjammu@gmail.com>, ddaaiimsbilaspur <ddaaiimsbilaspur@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, <dda@aiimsnagpur.edu.in>, Dy Director Administration AIIMS, Raebareli <ddaaiimsrbl@gmail.com>, Recruitment Cell AIIMS, Bathinda <recruitmentaiimsbathinda@gmail.com>, <ciso@aiimsraipur.edu.in>, <ciso@aiimskalyani.edu.in>, <anandchellappan@aiimsnaqour.edu.in>, <shivam.tsg@aiimsbhopal.edu.in>, <head.it@aiimsjammu.edu.in>, <rohit.bio@aiimsbibinagar.edu.in>, <drraje.path@aiimsmadurai.edu.in>, <drmohanraj@aiimsgorakhpur.edu.in>, <drabhyuday@aiimspatna.edu.in>, <raj.sharma@aiimsbhubaneswar.edu.in>, <Goyal.tarun@aiimsbathinda.edu.in>, AIIMS Gorakhpur <itcellaiimsgkp@gmail.com>, <draksharphc@gmail.com>, <itincharge@aiimsrishikesh.edu.in>, <aao@aiimsdeoghar.edu.in>, <mundraa@aiimsjodhpur.edu.in>, <debboruah@aiimsguwahati.ac.in>
Cc: RaviKumar RaviKumar <ravi.kumar89@gov.in>, ShriRajKumar Under Secretary <raj.kumar28@nic.in>, <arvind.thakur@nic.in>, <shalaka.kujur@nic.in>

Dear Sir/Madam,

With reference to the trailing mail, this is for your kind information and necessary action, please.

A Cyber Security Advisory has been issued regarding the recent security protocols and precautionary measures to be followed. You are requested to kindly review the advisory and ensure its implementation within your respective domain.

Please treat this matter as urgent and take appropriate action at the earliest.

--
regards,
Er.M.N.Mishra,
PMSSY,MoHFW,
Mob: 7982125857
---------- Forwarded message ---------
From: **Shri Raj Kumar Deputy Secretary** <raj.kumar28@nic.in>
Date: Fri, Jul 11, 2025 at 10:34 AM

441

Subject: Fwd: Cyber Security Advisory received From the National Critical Information Infrastructure Protection Centre (NCIIPC) reg.
To: mnmishramohfw <mnmishra.mohfw@gmail.com>, Ravi Kumar <ravi.kumar89@gov.in>, SUBHANSHU KUMAR <subhanshu.kumar@gov.in>

Deputy Secretary
PMSSY-I/ SNA
23063178

========== Forwarded message ==========
From: eHealth Section <telmed-mohfw@gov.in>
To: "Jaideep Kumar Mishra"<asfa-mhfw@nic.in>, "Roli Singh"<asfr-mohfw@gov.in>, "Ms. Roli Singh"<ash-mohfw@nic.in>, "Ms VHekali Zhimomi"<zhimomiv@ias.nic.in>, "oo.asphp Singh"<oo.asphp-mohfw@gov.in>, "Aradhana Patnaik"<asmd-mohfw@nic.in>, "UMESH KUMAR MISRA"<ofc.asme-mohfw@gov.in>, "Manashvi Kumar"<jstraining-mohfw@gov.in>, "G Latha"<g.latha@ias.gov.in>, "ELANGBAM ROBERT SINGH" <robert.elangbam@gov.in>, "Indrani Kaushal"<ea-mohfw@gov.in>, "gulam mustafa"<gulam.mustafa@nic.in>, "JS ME"<js.me-mohfw@nic.in>, "ANKITA MISHRA BUNDELA"<js-pmssy-mohfw@gov.in>, "Nikhil Gajraj" <nikhil.g@ias.nic.in>, "Vijay Nehra"<js-proc-mohfw@gov.in>, "Saurabh Jain"<js.policy-mohfw@gov.in>, "G Latha" <g.latha@nic.in>, "Vandana Jain"<vandana.jain@nic.in>, "Meera Srivastava"<jsrch-mohfw@gov.in>, "Vijay Sinha" <sinha.vijay@nic.in>, "Indrani Kaushal"<ea-mohfw@nic.in>, "Pradeep Khasnobis"<pradeep.khasnobis@gov.in>, "Rakesh Kumar Maurya"<rakesh.maurya@gov.in>, "Narendra Oza"<nk.oza@gov.in>, "KIRAN KARLAPU" <kiran.karlapu@gov.in>, "ROLI KHARE"<roli.khare@gov.in>, "Harsh Mangla"<harsh.mangla@ias.nic.in>, "SAROJ KUMAR"<saroj.kumar@nic.in>, "Sachin Kumar"<sachin.k@nic.in>, "SUSHIL Gahlaut"<sp.gahlaut@nic.in>, "Kumar Rahul"<kumar.rahul@nic.in>, "Gs Chitra"<gs.chitra@nic.in>, "Phool Prasad"<prasad-upsc@gov.in>, "Govind Kumar"<govind.bansal78@gov.in>, "RAJ KUMAR"<rkumar.edu@nic.in>, "RAKESH KUMAR" <rk.singh67@nic.in>, "PRIYADARSHIKA SRIVASTAVA"<priyadarshika.s@gov.in>, "Anjana Rajkumar"<director-cghs@cghs.nic.in>, "RAHUL KUMAR SRIVASTAVA"<rahul.srivastava@nic.in>, "R.K. Singh"<rk.singh27@nic.in>, "Indranil Das"<indranil.das@gov.in>, "Dinesh Kumar"<dinesh.kumar14@nic.in>, "Nikhil Agarwal" <nikhilkr.agarwal@nic.in>, "Poonam Meena"<poonam.22@gov.in>, "Mrs Bharti Sahai"<bharti.sahai@nic.in>, "Noorin Bux Khan"<noorinbux@ord.gov.in>, "ghalmevc"<ghalme.vc@gov.in>, "naveenaggarwal"<naveen.aggarwal@ias.gov.in>, "Nidhi Kesarwani"<nidhikesarwani@nic.in>, "Bherav Dutt"<bherav.dutt@nic.in>, "Samsul Haque"<samsul.haque@nic.in>, "DR.PULKESH KUMAR"<dr.pulkesh@gov.in>, "Z. A. Khan"<us-doj@mha.gov.in>, "Manoj Kumar Sinha"<mk.sinha26@nic.in>, "Sarvajit Kumar"<kumar.sarvajit@nic.in>, "G A Raghuvanshi" <gopal.aaditya@nic.in>, "Sarita Nair"<sarita.nair@gov.in>, "Shri Raj Kumar Deputy Secretary" <raj.kumar28@nic.in>, "Rajesh Kumar verma"<rajeshkumar.verma@nic.in>, "KAMAL ARORA DS" <kamal.arora@nic.in>, "abhijit cgca"<abhijit.cgca@gov.in>, "KAUSTUBH GIRI"<dsnhmfin-mohfw@gov.in>, "NAVEEN AGGARWAL"<naveen.aggarwal@ias.nic.in>, "Aashima Bhatnagar"<aashima.bhatnagar@gov.in>, "Arvind Thakur"<arvind.thakur@nic.in>, "RAJENDRA PRASAD SATI DEPUTY SECRETARY"<rp.sati88@nic.in>
Cc: "PUNYA SALILA SRIVASTAVA"<secyhfw@nic.in>, "Madhukar Bhagat"<jsehealth-mohfw@gov.in>, "HarishKumarJain PPS"<harish.jain68@gov.in>, "REENA SHARMA"<reena.sharma80@gov.in>, "Pawan Kumar" <pawan.kumar13@nic.in>, "Avinashyadav73"<avinash.yadav73@gov.in>, "eHealth Section"<telmed-mohfw@gov.in>, "ehealthmohfw1"<ehealth.mohfw1@gmail.com>
Date: Fri, 11 Jul 2025 09:56:22 +0530
Subject: Cyber Security Advisory received From the National Critical Information Infrastructure Protection Centre (NCIIPC) reg.
========== Forwarded message ==========

Sir/Madam,

Kindly refer to the attached Cyber Security Advisory received from the National Critical Information Infrastructure Protection Centre (NCIIPC). This is for your information and necessary action, please.



Regards
eHealth Section

442

Ministry of Health & Family welfare
Room No.-213, D-wing, Nirman Bhawan
New Delhi-110011
Tel No.-23062263

14 attachments

Advisory No- TA-TAG-2025-07-09-002- Abuse of Exchange Impersonation Capabilities of Microsoft Exchange Servers [TLP- AMBER].pdf
340K

Advisory No- TA-MI-2025-07-09-002- Malicious IOCs Targeting Critical Sectors [TLP- AMBER].pdf
290K

Advisory No- TA-PHI-2025-07-09-003- Phishing Attack [TLP- AMBER].pdf
325K

Advisory No- VA-2025-07-09-010- Critical Vulnerabilities in Multiple Products [TLP- CLEAR].pdf
310K

Advisory No- TA-TAG-2025-07-09-001- Threat Actor GrayAlpha [TLP- GREEN].pdf
425K

Advisory No- TA-MAW-2025-07-09-010- Qwizzserial Android Malware [TLP- CLEAR].pdf
627K

Advisory No-TA-MAW-2025-07-09-008- ACR Stealer [TLP- CLEAR].pdf
318K

Advisory No- TA-MAW-2025-07-09-009- XtremeRAT [TLP- CLEAR].pdf
306K

Advisory No- TA-MAW-2025-07-09-007- MooBot Malware [TLP- CLEAR].pdf
618K

Advisory No- TA-MAW-2025-07-09-006- GIFTEDCROOK Infostealer [TLP- CLEAR].pdf
344K

Advisory No- VA-2025-07-07-006- Active Exploitation of Vulnerabilities in Ivanti Endpoint Manager Mobile [TLP- GREEN].pdf
630K

Advisory No- VA-2025-07-07-005- Critical Vulnerabilities in Multiple Products [TLP- CLEAR].pdf
357K

Advisory No- TA-APT-2025-07-07-001- APT36 Campaign [TLP-GREEN].pdf
323K

Advisory No- TA-MAW-2025-07-08-005- Threat Actors Developing Cracking Websites for Stealer Malware Distribution [TLP- GREEN].pdf
660K

Fwd: Advisory No: TA-TAG-2025-07-09-002: Abuse of Exchange Impersonation Capabilities of Microsoft Exchange Servers [TLP: AMBER]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Wed, 09 Jul 2025 5:08:13 PM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

---------- Forwarded message ----------
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Wed, 09 Jul 2025 15:33:17 +0530
Subject: Advisory No: TA-TAG-2025-07-09-002: Abuse of Exchange Impersonation Capabilities of Microsoft Exchange Servers [TLP: AMBER]
---------- Forwarded message ----------

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-TAG-2025-07-09-002

Cyber Security Advisory: Abuse of Exchange Impersonation Capabilities of Microsoft Exchange Servers

This data is to be considered as TLP: AMBER

It has been observed that threat actors are actively targeting administrative accounts assigned the "ApplicationImpersonation" role on Microsoft Exchange servers (versions 2010, 2013, 2016, and 2019) to gain unauthorized access to user mailboxes. This access is being leveraged to conduct malicious activities, including email exfiltration, internal reconnaissance, and privilege escalation. The "ApplicationImpersonation" role permits access to designated mailboxes while bypassing standard role-based access controls, thereby making it a high-value target for attackers. Although the exact initial access vector remains under investigation, likely causes include credential

compromise, misconfigured permissions, or the exploitation of an undisclosed vulnerability within Exchange services or associated authentication mechanisms.

Impact:

- Unauthorized Mailbox Access: Attackers can read and exfiltrate emails from any user.
- Data Leakage Risk: Sensitive business, legal, or financial information can be stolen or exposed.
- Business Email Compromise (BEC): Adversaries may impersonate users to conduct fraud or phishing.
- Lateral Movement Opportunity: Stolen credentials can be used to access other internal systems.
- Regulatory and Reputational Damage: Breaches may trigger compliance violations and loss of trust.

Recommendations:

- Enable mailbox auditing and EWS access logging.
- Audit and Review all accounts with "ApplicationImpersonation" role and administrator privilege. Enforce least privilege: only assign impersonation to specific, tightly-scoped applications.
- Restrict remote PowerShell access to specific IPs or roles.
- Implement network segmentation and firewall rules to limit internet-facing Exchange exposure.
- Enforce Multi-Factor Authentication (MFA) for all admin and service accounts.
- Use dedicated admin accounts (not shared or used for daily tasks).
- Privileged Access Management (PAM) may be considered and monitor access to Exchange role

References: CERT-IN [CMTX-P072025502]
https://learn.microsoft.com/en-us/exchange/client-developer/exchange-web-services/impersonation-and-ews-in-exchange
Note: TA-TAG: Threat Alert Threat Actor Group

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: AMBER. Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.
Disclaimer:
The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

advisory@nciipc.gov.in mailing list


2025
International Year
of Cooperatives
Cooperatives Build
a Better World
SANCHAR SAATHI
MOBILE APP

Fwd: Advisory No: TA-MI-2025-07-09-002: Malicious IOCs Targeting Critical Sectors [TLP: AMBER]

Madhukar Bhagat < jsehealth-mohfw@gov.in >

Thu, 10 Jul 2025 9:35:07 AM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

---------- Forwarded message ----------
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Wed, 09 Jul 2025 16:29:15 +0530
Subject: Advisory No: TA-MI-2025-07-09-002: Malicious IOCs Targeting Critical Sectors [TLP: AMBER]
---------- Forwarded message ----------

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-MI-2025-07-09-002

Cyber Security Advisory: Malicious IOCs Targeting Critical Sectors

This data is to be considered as TLP: AMBER

Based on analysis, please find below malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

**********IOC START**********
IPs:

179[.]43[.]173[.]12
43[.]153[.]20[.]43
167[.]172[.]6[.]243
87[.]121[.]84[.]34

170[.]106[.]147[.]35
144[.]172[.]115[.]127
117[.]209[.]84[.]223
220[.]158[.]234[.]135
160[.]187[.]246[.]7
95[.]214[.]53[.]84
120[.]85[.]119[.]22
5[.]79[.]105[.]22
27[.]47[.]0[.]24
192[.]169[.]7[.]221
122[.]252[.]224[.]101
45[.]115[.]89[.]240
45[.]135[.]193[.]162
27[.]43[.]205[.]186
45[.]135[.]194[.]11
223[.]149[.]203[.]190
146[.]190[.]115[.]115
175[.]107[.]1[.]84
120[.]85[.]182[.]239
45[.]8[.]145[.]203
103[.]70[.]167[.]26
45[.]115[.]89[.]153
120[.]85[.]116[.]199
112[.]94[.]98[.]198
27[.]43[.]206[.]157
27[.]43[.]204[.]62
117[.]235[.]57[.]48
58[.]44[.]132[.]214

URLs:

hxxp://45[.]230[.]66[.]100:10989/
hxxp://115[.]54[.]237[.]0:34245/
hxxp://103[.]167[.]204[.]107:44930/
hxxp://182[.]235[.]20[.]234:44650/
hxxp://83[.]177[.]223[.]182:37749/
hxxp://117[.]209[.]88[.]154:57970/
hxxp://89[.]67[.]72[.]83:52845/
hxxp://113[.]230[.]63[.]19:57517/
hxxp://45[.]116[.]121[.]211:49511/
hxxp://117[.]244[.]79[.]53:33366/
hxxp://59[.]97[.]181[.]93:43520/
hxxp://117[.]209[.]91[.]22:57945/
hxxp://125[.]41[.]223[.]184:59237/
hxxp://117[.]244[.]236[.]207:41139/
hxxp://61[.]70[.]84[.]40:55300/
hxxp://61[.]1[.]218[.]176:47600/
hxxp://61[.]52[.]130[.]192:56399/
hxxp://103[.]208[.]105[.]148:49896/
hxxp://112[.]198[.]130[.]112:49467/
hxxp://115[.]63[.]53[.]21:34080/
hxxp://45[.]230[.]66[.]108:11492/
hxxp://103[.]83[.]145[.]108:34151/
hxxp://45[.]230[.]66[.]121:10380/
hxxp://45[.]230[.]66[.]109:11337/
hxxp://45[.]230[.]66[.]117:10479/Mozi[.]a

hxxp://175[.]30[.]69[.]76:34973/Mozi[.]a
hxxp://27[.]210[.]218[.]95:60630/Mozi[.]m
hxxp://222[.]140[.]133[.]30:34163/Mozi[.]m
hxxp://182[.]235[.]148[.]10:46021/Mozi[.]m
hxxp://182[.]113[.]195[.]144:56549/Mozi[.]m
hxxp://123[.]12[.]199[.]141:53982/Mozi[.]m
hxxp://112[.]248[.]245[.]75:35632/Mozi[.]m
hxxp://27[.]204[.]227[.]48:42701/
hxxp://103[.]208[.]230[.]97:45985/
hxxp://77[.]52[.]247[.]37:37730/
hxxp://183[.]35[.]50[.]67:39917/
hxxp://117[.]211[.]38[.]253:44595/
hxxp://139[.]5[.]11[.]182:54381/
hxxp://71[.]207[.]128[.]92:39211/
hxxp://45[.]230[.]66[.]117:10224/
hxxp://45[.]230[.]66[.]111:11736/
hxxp://45[.]115[.]89[.]206:60805/
hxxp://45[.]115[.]176[.]177:56201/
hxxp://42[.]235[.]0[.]47:47047/
hxxp://39[.]86[.]40[.]180:53433/
hxxp://219[.]77[.]137[.]52:54514/
hxxp://175[.]107[.]3[.]215:52341/
hxxp://120[.]28[.]195[.]47:59054/
hxxp://117[.]235[.]147[.]226:43820/
hxxp://112[.]240[.]200[.]125:48954/

**********IOC
END**********

Recommendation:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.

Note: TA-MI: Threat Alert Malicious IOCs

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: AMBER. Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Disclaimer:
The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

advisory@nciipc.gov.in mailing list



450

Fwd: Advisory No: TA-PHI-2025-07-09-003: Phishing Attack [TLP: AMBER]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Thu, 10 Jul 2025 9:36:22 AM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Wed, 09 Jul 2025 17:19:29 +0530
Subject: Advisory No: TA-PHI-2025-07-09-003: Phishing Attack [TLP: AMBER]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-PHI-2025-07-09-003

Cyber Security Advisory: Phishing Attack

This data is to be considered as TLP: AMBER

It has been observed that government personnel have received phishing emails from spoofed/compromised email IDs and malicious domains. The email contains a hyperlink "hxxps://authentication.elevations[.]world/important.shtml?modes=NjkmJE44NilVOSZBQThGRSA7NjVBK0Y9Tz1CWUk7QCAgs://lserver.roots-enargy[.]com/zrswtiknaa.html?ytpsmivqmg=info@adencont[.]com", with button "Resolve Message (10)". Upon clicking the button "Resolve Message (10)" , it opens a cloned phishing page of an autofill email ID of a particular email ID. The IP address and domain involved are malicious and currently active, potentially compromising the user credentials/propagating malware payload.

**********IOC
START**********

Url:
hxxps://authentication.elevations[.]world/important.shtml?modes=NjkmJE44NilVOSZBQThGRSA7NjVBK0Y9Tz1CWUk7QCAgs://lserver.roots-enargy[.]com/zrswtiknaa.html?ytpsmivqmg=info@adencont[.]com

Domain:
elevations[.]world

IP:
104[.]21[.]1[.]187
**********IOC
END**********

Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Install and regularly update antivirus software.
- Conduct regular backup practices and keep those backups offline or on a separate network.
- Implement Multi-Factor Authentication (MFA).
- Never click and execute email attachments from unknown sources.
- Never run unknown files with exaggerated titles.
- Users of nic.in and gov.in domains be sensitised about the threat vector.

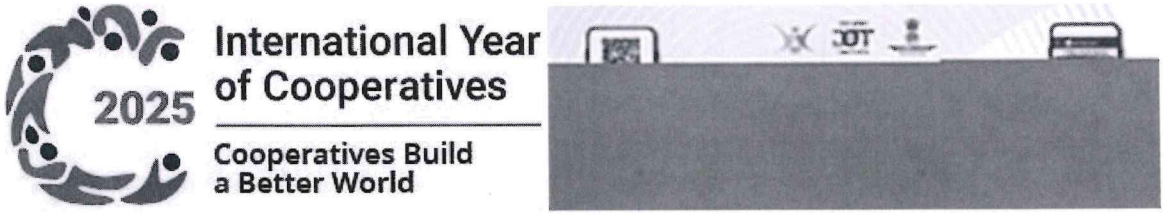
Note: *TA-PHI: Threat Alert Phishing Advisory*

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: AMBER. Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Disclaimer:
The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

advisory@nciipc.gov.in mailing list


2025
International Year
of Cooperatives
Cooperatives Build
a Better World

Fwd: Advisory No: VA-2025-07-09-010: Critical Vulnerabilities in Multiple Products [TLP: CLEAR]

Madhukar Bhagat < jsehealth-mohfw@gov.in >

Thu, 10 Jul 2025 9:36:47 AM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Wed, 09 Jul 2025 17:05:33 +0530
Subject: Advisory No: VA-2025-07-09-010: Critical Vulnerabilities in Multiple Products [TLP: CLEAR]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: VA-2025-07-09-010

Cyber Security Advisory: Critical Vulnerabilities in Multiple Products

This data is to be considered as TLP: CLEAR

Vulnerability in SAP NetWeaver Enterprise Portal Federated Portal Network
A deserialization of untrusted data vulnerability has been discovered in SAP NetWeaver Enterprise Portal Federated Portal Network that could potentially lead to a compromise of confidentiality, integrity, and availability of the host system. An attacker can exploit this vulnerability to take control of an affected system.
CVE-ID: CVE-2025-42980 (Critical)
Reference: https://support.sap.com/en/my-support/knowledge-base/security-notes-news/july-2025.html

Vulnerability in SAP S/4HANA and SAP SCM Characteristic Propagation
A code injection vulnerability has been discovered in SAP S/4HANA and SAP SCM Characteristic Propagation that could potentially lead to a compromise of confidentiality, integrity, and availability of the host system. An attacker can exploit this vulnerability to take control of an affected system.

CVE-ID: CVE-2025-42967 (Critical)
Reference: https://support.sap.com/en/my-support/knowledge-base/security-notes-news/july-2025.html

Vulnerability in SAP NetWeaver XML Data Archiving Service
A deserialization of untrusted data vulnerability has been discovered in the SAP NetWeaver XML Data Archiving Service that could potentially lead to a compromise of confidentiality, integrity, and availability of the host system. An attacker can exploit this vulnerability to take control of an affected system.
CVE-ID: CVE-2025-42966 (Critical)
Reference: https://support.sap.com/en/my-support/knowledge-base/security-notes-news/july-2025.html

Vulnerability in SAP NetWeaver Enterprise Portal Administration
A deserialization of untrusted data vulnerability has been discovered in SAP NetWeaver Enterprise Portal Administration that could potentially lead to a compromise of confidentiality, integrity, and availability of the host system. An attacker can exploit this vulnerability to take control of an affected system.
CVE-ID: CVE-2025-42964 (Critical)
Reference: https://support.sap.com/en/my-support/knowledge-base/security-notes-news/july-2025.html

Vulnerability in SAP NetWeaver Application server for Java Log Viewer
A deserialization of untrusted data vulnerability has been discovered in the SAP NetWeaver Application server for Java Log Viewer that could potentially lead to a compromise of confidentiality, integrity, and availability of the host system. An attacker can exploit this vulnerability to take control of an affected system.
CVE-ID: CVE-2025-42963 (Critical)
Reference: https://support.sap.com/en/my-support/knowledge-base/security-notes-news/july-2025.html

Vulnerability in Frauscher Sensortechnik GmbH Products
An Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability has been discovered in FDS101, FDS-SNMP101 and FDS102. The affected versions are FDS101 <= v1.4.25 , FDS-SNMP101 <= v.2.3.9 and FDS102 v2.8.0 < v2.13.3. An attacker can exploit this vulnerability to take control of an affected system.
CVE-ID: CVE-2025-3626 (Critical) CVE-2025-3705(Medium)
Reference: https://certvde.com/en/advisories/VDE-2025-030/#cvedetails-CVE-2025-3705

SAP Released July 2025 Security Notes
SAP has released security notes to address several critical vulnerabilities affecting multiple products. An attacker can exploit these vulnerabilities to take control of an affected system.
CVE-ID: CVE-2025-30012 (Critical), CVE-2025-42959 (High), CVE-2025-42953 (High), CVE-2024-53677 (High), CVE-2025-42952 (High), CVE-2025-42977 (High)
Reference: https://support.sap.com/en/my-support/knowledge-base/security-notes-news/july-2025.html

Note: *VA: Vulnerability Advisory*

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: CLEAR. Recipients can spread this to the world, there is no limit on disclosure. Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction.

Disclaimer:
The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

advisory@nciipc.gov.in mailing list


2025
International Year
of Cooperatives
Cooperatives Build
a Better World

Fwd: Advisory No: TA-TAG-2025-07-09-001: Threat Actor GrayAlpha [TLP: GREEN]

Madhukar Bhagat < jsehealth-mohfw@gov.in >

Thu, 10 Jul 2025 9:37:56 AM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Wed, 09 Jul 2025 15:18:49 +0530
Subject: Advisory No: TA-TAG-2025-07-09-001: Threat Actor GrayAlpha [TLP: GREEN]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-TAG-2025-07-09-001

Cyber Security Advisory : Threat Actor GrayAlpha

This data is to be considered as **TLP: GREEN**

It has been observed that GrayAlpha, a financially motivated threat actor, utilising advanced tactics, tools i.e. fake browser update pages, fake 7-Zip download sites & the Traffic Distribution System (TDS) TAG-124 and infrastructure to deliver malware. Adversary uses custom PowerShell loaders such as PowerNet, which decompresses and executes NetSupport RAT and MaskBat, a more obfuscated variant of FakeBat. These custom loaders demonstrate the group's sophistication and ability to adapt, obfuscate their tools and evade detection. The persistent use of these evolving methods, alongside the continued reliance on TAG-124, marks a significant step in their adaptive and persistent attack strategies.

Key Findings:

- New Infrastructure: GrayAlpha operates using new domains and additional IP addresses for payload distribution, leveraging a variety of custom tools for malware delivery.
- Custom Loaders: Two custom PowerShell-based loaders, PowerNet and MaskBat, have been identified, with PowerNet executing NetSupport RAT and MaskBat being an obfuscated variant of

FakeBat.

- Infection Vectors: Primary infection methods include fraudulent browser update pages, fake software download sites (e.g., 7-Zip), and TAG-124, a new traffic distribution system.
- Active Infection Methods: Fake download pages for 7-Zip remain active, with newly registered domains.

**********IoCs START**********

IPs:

45[.]89[.]53[.]243
5[.]180[.]24[.]50
85[.]209[.]134[.]64
154[.]216[.]20[.]106
94[.]131[.]101[.]65
86[.]104[.]72[.]19
141[.]98[.]168[.]106
77[.]90[.]38[.]106
89[.]105[.]198[.]190
5[.]252[.]178[.]150
5[.]252[.]176[.]143
45[.]89[.]53[.]110
103[.]35[.]188[.]97
85[.]209[.]134[.]45
94[.]159[.]100[.]117
103[.]113[.]70[.]142
94[.]159[.]100[.]111
86[.]104[.]72[.]208
45[.]88[.]91[.]8
195[.]133[.]67[.]165
2[.]58[.]95[.]73
103[.]35[.]191[.]28
86[.]104[.]72[.]23
188[.]132[.]183[.]172
85[.]209[.]134[.]137
74[.]119[.]194[.]151
138[.]124[.]184[.]64
85[.]209[.]134[.]186
138[.]124[.]183[.]175
176[.]32[.]39[.]71
62[.]76[.]234[.]99
38[.]180[.]141[.]203
45[.]89[.]53[.]60
138[.]124[.]183[.]79
94[.]159[.]96[.]222
185[.]125[.]50[.]209
188[.]124[.]59[.]18
91[.]149[.]232[.]112
103[.]35[.]191[.]137
212[.]224[.]107[.]150
193[.]23[.]118[.]165
103[.]113[.]70[.]37
62[.]60[.]155[.]194
194[.]87[.]82[.]252
38[.]180[.]142[.]198
45[.]140[.]17[.]49

458

62[.]76[.]234[.]49
138[.]124[.]183[.]95
103[.]35[.]190[.]215
193[.]32[.]177[.]223
86[.]104[.]72[.]16
91[.]228[.]10[.]81
85[.]209[.]134[.]209
103[.]113[.]70[.]158
138[.]124[.]183[.]176
91[.]200[.]14[.]23
166[.]88[.]159[.]187
45[.]82[.]84[.]13
103[.]35[.]191[.]222
85[.]209[.]134[.]188
206[.]206[.]123[.]97
138[.]124[.]180[.]85
138[.]124[.]184[.]214
62[.]76[.]234[.]234
172[.]208[.]117[.]89
45[.]89[.]53[.]215
103[.]35[.]190[.]40
38[.]180[.]80[.]124
85[.]209[.]134[.]106

Hashes:

4d0663cff0c5c3f29c81e9aefd37f16a318ff638986ecc60e9bce6c90b72606b
0e71728e5e6a762923fc0372e2047e0d969bcc5efbf4f3010df2ff6576cab725
ebfdea1721914a504465ea474edc3f823c3e13fc71c86f04f4793c61e5070d92
ebfdea1721914a504465ea474edc3f823c3e13fc71c86f04f4793c61e5070d92
2938261c867331e12e7cff9ee28366f3986986108eeb00507db74cf0d7b6aad2
c220f9ba0ee8445ab6d36f19d7cf24fd6df72eea41b9ba40f585451ee24c0f6d
9a4e39fcb4033a9c849890085b67faea7265eaf56744e77aa8180b1834b7e14a
d0add7a41b8c78ab0134752665278b9544d417b244a788c620c5da5215b515c0
5072735b87e62c0239099fcd3d74a677e1b4c6497e0b17ed8ea4c83778c13039
aadf323d8052da80c761ab9d05717603804405ee33e624926009a30d857d6d1a
36b79a3eca6d0ee23daf10c436f4ec5c8c279fbfd79c965c7e37515c148c3c5b
401c5d2157d303df1ca465ff4097ee4474574c39f614cbb5734193a3917354c0
4665c7b360b18496be00246eb3bc886e83b22028e95156101bf73bf0c48dddd3
056451b28c4bfe6bf1536c1d67b33f312a06c656cd3c633f40cc5f5b85c6528b
6b999462e434b258980b1532f5d0c3661646f7bb9567aecdd748f6be10dcb740
0c8b9fa67d1d149636b560a2ec8f9c50cd41ebf11f5691cf2ea39f1d057f8ff1
0c8d22d58a747ceccad56317b9c0afe58fe4b9f3c2138134e978e43a5f5ac390
e2c283438e5f9236c5cb2e6b8b95ca78d520f7b776d64a050664972cb51076f5
a5febb4b5ba6572594de87d2a9de6df65d49da755385bf3d3d4d054772ce493c
c3ecbc6023bfa170c31eaf7033b68495798e305111ca9f2f203f58b9ec942384
8246ba12e1ebfcdbaed80a7ba1ec65423f23b9b7820c0dfb07ee38baa83d6a20
1f38a9e17e5096bca84b6ec87eb5470b2ce4450a6a03b3e41b38dbd91ab281da
e9010ab2a031125f12225d8b1f19ac65bc03b87332dc5caa35028a577b9ca0fe
f4052e52fed661fd05ea39a5187781ec6c234c5d7ea4ab91cd77f2e1d2c709b5
5e9362dba53021ab588e396e1cb28100718471f07c5dd5cafa6bf5728f014b97
13265c0e32312a0763f3f8fed0f017a606355987ac9398bfb38f47c760ad32b0
41be156c27dad780dd96493319dbd89228616573ec7d731ca2e642ee0e554af3
58cb66268b58d7ca77fb5f5df668ffa76a23854a6267914fc3973dbf92394612
8d5d4e48ce623085efec9a56981b0ab74f1180f3b42614df88f11da543f2849a
c5fa7fd1ff45c5cfaec851795f4c2e15326046f3022778bdf6f37b7b1dd75f5c
c6e672b832dcf78490ea8d128f5f8a647274b9b98d851bc36ff07b2d3a0d7ba3
191a8766da98b1f992072045905cf82c771d8cb9f697d08873686778dc70c7f6
982ec3915d458007e960a4dbe0c9c914825fd88c1739ab3f7edfebaaa10bc265
710e80fb64e08f20ab58c20ccdbc966f6e3b54511775e8ed99ff0bcf51690227
4814ea15da1826d9ef400c3e607ca87d11b18b8a1b4f43f13afa93467429dfb8
952cac8ec226b4ed38a2631c220bb80409edbc0c9a0ac2793b879a259172282b
c220f9ba0ee8445ab6d36f19d7cf24fd6df72eea41b9ba40f585451ee24c0f6d
f491d8b510ee283d24d40aa5233743d8cf834a164d0f681af8870dd1f35b734c

a67d73996a5479312f4a4ea4fccdde293695359aa6b6da06c01248066a7131f9
194d739fa93970d63dade70aae7c3b9ac8a6938be9f0e2d470d3adf8c106bfad
3c6dacad931bf24eb953858c0bb3e49fe821d111d9003c9fffcb814ae6e8edf8
65b601f8154bddd42cb31ce166697335e79f2e713655865bee66654c51e7c1dc
b417396efb07943d380182d610da313607308a74fc0dc77318407a5248cbab6e
81e6adebca376dfbda0484ab4475d0ac76a1e86afe0930e45ab7137cfd378d38
4b268cfbdb86017f6271f09eb2aa54334de24d0ed12cfeb26fbb3dd8e104a8d3
8d8d21f2c28f3e44b7253583e04d11cf7e7453dab139c187201f80e70d89b579
8684e74d35baab30e8f8af7db486c2a339d3063feb2074109b8c96c1fea8313e
8684e74d35baab30e8f8af7db486c2a339d3063feb2074109b8c96c1fea8313e
6053d67835d2925c52263bdb9e4d7475e1015ea9cc4c8f994cfa7e0dbdb7e27f
52ef3b610426343314e6c0f238e4460f0dffedbd022d33cb8f8e78e980d604e0
52ef3b610426343314e6c0f238e4460f0dffedbd022d33cb8f8e78e980d604e0
50b102938d29cc7f61c67da6981545c69f70c7178d009ec1999ee0ddfe81ebba
974285914961125d2963435c3dbe49b882cd88d95563b1ae3a62cd6240618c16
a309753efca5242bbc9ca0e54a381ef2bac6625a0f591d79f8525e1ec196be4e
1ec930716999f6a80a4f32624d8f907f2c7887e15b1c518d22f4aefe49367bba
c902a206da5c3e1a4b8b8ba9f0e63f314e8cadcf044c25f729176b29c19bcbbb
8515d46da83fb649db969b2acca47cd10f232174af358560210b362a56594fd1
908ef89767bcd583edb96a8c12f3046b9db522cc7310e2c20799881d7bf75f9d
da43703c733a1b0af183fdb61877b5c15651c21ffcc3a49c6addc83d76c10329
91c2fbc594469839ad062e7cf359f2451fe8a14f041d8afe515ceab800c35133
fbe1970d89b8546cd57522bf479e8be08fec4f3df9bdf79d0f3436250ce38379
76f98321f50595725f64f058d8f33103d518c5d77680fd7d5521c41786299358
e4fff1e153ef46a29865f28df724e7a3246809d9ae75a7546b580938acbbcb73
184a400fe334027ff287ad0cf83c165fdf4605507c83ec054fb2b544f877163c
ee6a58d1e3ce4f2e7fac7bb3c1f1c24836bcc79f456035aede52b7d14a7de77f
1d17937f2141570de62b437ff6bf09b1b58cfdb13ff02ed6592e077e2d368252
890cf9827361add4c2a6e5b93f7f9ccc9bb2f555e0cd535de144203f7156a959
3869340562136d1d8f11c304f207120f9b497e0a430ca1a04c0964eb5b70f277
bdd89826ab8d3e3c03833b1ea8e4b0a34c80f13bfa5882e5b82f896cec41d141
c3dc66c657dd5a8a624c6eba67a6b8d1dada8ceeb13aab169c3a88c615831560
ae4db4f97700aab607368a4d3a489215b2ddb5af60004b8da6e5b0c0220c2c25
94bb5b8cc0a2d01d4f65294c816299b97dd38bc7be8fc9089dc90cc969995528
8b7be1efcddddc3a29ae0514a6ae758e7f86be193ffe380e5e1e38dc22affb38
e300c44b45b07f3766586e500f4f3596c23ffd80171eaa5334bb4db3e8d027e0
41c671332b58f92187e32771ed1ba86c1ed256e36f036f74c91cf1aa7db07bc2
f015da1f2ada32f734b81aa282bea62840cd84afaa353ca52d5e2d0c82e705d1
c2f1c765b03b4ae0c08455c2b5e917ba8564ad945c3580a1e622169aad67807a
f4f02429e8e1e966203d69610c31ae94ad4d34de10efd5edc4669ce067c4de4f
3bdaa78077bd71e40b62ec2d6797c027f0b8deba9c3a7de9eb22823ad05c8201
4d03c2a47265eab0c87006a4a2965fcf394fbdabb8e86cbe16b36376d04b8143
b3f46a63817a2076e3de49957d5801eb8ede9dc1498bdab702fcc6f8cccf0e61
50a5e6a357c841e6c2058ee658c70756da4b803f2a4f6d2cf96ab882a03a5294
809b54b0f6092cad1a764872acb9a31ed99792589b84cdb279b4b1d15e8ec8e2
de5f6cc6a3eaee870f438a43e1e262283124aa1cfa11ad395a05c4bff026c09f
809050c6f29e80e9d0918060634df601ae12b27cc50439f4c123b6301ce26043
1e54b2e6558e2c92df73da65cd90b462dcafa1e6dcc311336b1543c68d3e82bc
2ba527fb8e31cb209df8d1890a63cda9cd4433aa0b841ed8b86fa801aff4ccbd
9953bbe13394bc6cd88fd0d13ceff771553e3a63ff84dc20960b67b4b9c9e48e
5303183d82b8c4d2a47fab4167868a8cfbf8d56d3397701ab890e88c99105ae4
bfc1064d3624c7bc68ef6b8ce2b0f40229d5981472c8b443c58f38bf3f461b2a
acbed908bc3e804ad183f3598dfb379a366f6209462f5fffc77fc9231ae1b048
2fd9e14830bbeef24fdff29a850a6164af4c4722d742185e022df9106029b587
bfc1064d3624c7bc68ef6b8ce2b0f40229d5981472c8b443c58f38bf3f461b2a
1367dcf619cb935dc08d349fc18d3f9726cfceff151f4d57beff45591712189c
f10bd5443148d47fbf7c6a6998651eb9bda4c7c9213f9e5a65a76e98637cb748
2bd6b5cbeddab8b01e14ed4c073afdbd4316340aada77e3e55ba5e1af21652f7
881a84477b509e2e63b70915055b9af1d12cf8fde9fb5031823c8c2a38c8979a
acbed908bc3e804ad183f3598dfb379a366f6209462f5fffc77fc9231ae1b048
de88ae471d8b95e5e10264aea5eb040fedb9bb71428385e7cff6c77a6ae47d97
a98d6df438ba2615107642c7c6da104de1c9aefdb0f184aead763ae3057c11e9
af3530b841049f90b9f5c818910f1877ef8f89bea0454fe72ada397e9bef1565
37990aecf5fecc61e4b3a3f5eaec14c8ed03cb20681dc53c367d5541600f9312
08d4a681aadff5681947514509c1f2af10ff8161950df2ae7f8ee214213edc17
c8d9270a38a2e6e0659b6b9aab7543add0d1bc521afb51f7dcf68c7426a8d57e
d6fce7c094994b19d96c9ebcccc07b9fb5efda2e4e1da352d9e0e031f0457c5e
547ef48f46ecfe31ee7edc7bbff0c2406f43d11915bcef84372172873012eacd
3cfcb57b94e69372cd2815dc63d66ab4b4ac4fec48b3b092f76ae5c9beaa353f

460

69d267234d62fd6ffd1c6a12b36835b1454dce4a6df1b370e549e275961ae235
ade52759c6aba1a0aa5b0dd3f779064c1021502bbe944dd704214522fc66707e
a03badf094c46a97711da1494749962168472550f786dbea508cf6978252a2c8
8719ccdb87c8b2c4e312208bd17a8df42a1683c10bb32699bb415a66f0dbdda0
8719ccdb87c8b2c4e312208bd17a8df42a1683c10bb32699bb415a66f0dbdda0
139b48d1b94a9c31a4c7ac1feaa7bf54b50f33ab8936f22404648233bf48cc95
878a3a06aadf6d22a61dc6a160a389b6fd34f6629a32df3407c300bcd7829f4b
b7b7516063052b84f3d240b66630b01d0c098376dba531c5ae9dbcaa1a099820
e77bd0bf2c2f5f0094126f34de49ea5d4304a094121307603916ae3c50dfcfe4
127c691f5a354fa0933ec3e9d9d1bb976c2de7092065d75ea66626c8dc007029
bc5c7fc357244b8cdb1d79c545c4ac5d20ba770d028dd4bc66a00dd4ba2679fa
b3a95ec7b1e7e73ba59d3e7005950784d2651fcd2b0e8f24fa665f89a7404a56
3802c396e836de94ee13e38326b3fb937fcf0d6f6ef9ccdf77643be65de4c8ee
7363086b152422c99618377e384874a17a708d9eb217c0a7c6f8b6f3216f1e4c
63629c87fe460abb657a504bb9786b913b1250288681520cee9e9fbcb14e888f
c399fe7ba04828aeadd881d7daa17dc0e3b880e95cc1aa2295c510f6bd8aa1d4
4c2f8feced7768f756ac7d4fa633b08fd61f0ba198c860fa4f1093dedbf060d2
5838f38e80657dd318bdbcfd1bdb87181e527f2125185ce95b43abd02badea86
802338ddade5c023b83dd2111fe30b7d5b4b21b86408e91544345e0c45702a1d
2c59f3552a77d2c9527970ae99e204ec279756ac24815a899ab43356420057e7
902c9aba42378c40c6c9623bab2326cb8b98fa06cfc0ee0379349055137c9500
e580dd04cbe2407ac7ab06d148297231cffbb8f8f986ce1e152383970927bb71
84f2d273623efb6cdd126a89c1f9567e8977d21ffe684758dd722a27d2d53aa9
ff6d88f53f2a08107c08729f2698f75cc759f3c423fe6e5b99b2c32d7c40f8a4
d73af3bd70f0f68846920d61fab8836cf8906a2876489801f6e130f4d92aa50d
9112b8623844774b056c842da3417f75c86bff115d5d15db2d6226c6ffd98895
0ddce15bea228c65d3b456759de0abc87aa6e805fd6c466347e9b76913a538ce
381c6f7f8c12ea1ac483dad9ac71c09fa807bd1ffe2479f6d6c7da14013e7899
62242df8c7db337e46f44c4323ac9738adba89f095deb8e5d873ee8b35fa5079
f10ecfd0ac437420e8754dbefd9b49c710fe87548ec1350eb2598785b33afec1
bc3f10302a62a5e100a2a31e50a9c32a554d74015f17be2299273d143d2b42de
4f71162cef29a8b7feb56574b99c0eccd82c39d226b408c1e7233971588edee5
58ab8b2a21e33b0700d11efd5a677bd98e536e200b45e22aa06059c1088063f7
96dfb6337647d890875919334a8dfc1f8f6e887f4b9ff6afedfb3574c7b444a3
0c46fd6353f75a8dec81adca9f35e839bd8a7ac9490b947374e3c1e3b24e0f79
50cbf5b9ce69a5c9f9adaf59bf53f4f0609afcba36826e2fa88ca6cedbc06e7a
1f52416232bf57e6cbd8a72335a5f321cf8a571e53b043ee69dc3647d4978844
5303183d82b8c4d2a47fab4167868a8cfbf8d56d3397701ab890e88c99105ae4
73e775fc0e1a4780a06fda4f21cca16c1dd9eda57fc8a0ab4fb14ebe5a259eac
a38f1ccf9d3e29e39fcb01b53fc245eac2128c4219c6567891dba4f6529f98c1
acbed908bc3e804ad183f3598dfb379a366f6209462f5fffc77fc9231ae1b048
acbed908bc3e804ad183f3598dfb379a366f6209462f5fffc77fc9231ae1b048
e8c56706296175195a03348b9cd5064e60c36fdeaa6e5fd7b5614ca6bca1c3f8
abd4263c97ab33b22f67e581ebb09ec7b98e4084dd32a7eca6502d3737715769
1367dcf619cb935dc08d349fc18d3f9726cfceff151f4d57beff45591712189c
1367dcf619cb935dc08d349fc18d3f9726cfceff151f4d57beff45591712189c
2bd6b5cbeddab8b01e14ed4c073afdbd4316340aada77e3e55ba5e1af21652f7
1c6c79b07e45630debe31362e4c89ffab3560c4712470f7af891bb31539d153a
acbed908bc3e804ad183f3598dfb379a366f6209462f5fffc77fc9231ae1b048
acbed908bc3e804ad183f3598dfb379a366f6209462f5fffc77fc9231ae1b048
e9b0cc2118a7a07709b56f7358c07f4a2959f81c87da5f565fa08382768fac8b
e8c56706296175195a03348b9cd5064e60c36fdeaa6e5fd7b5614ca6bca1c3f8
2bd6b5cbeddab8b01e14ed4c073afdbd4316340aada77e3e55ba5e1af21652f7
a38f1ccf9d3e29e39fcb01b53fc245eac2128c4219c6567891dba4f6529f98c1
0d44ff778dbecf8d951c54c199bd35ba0fe5ac817d5ef61b2fe998dfdb794560
34f50a5215c544cbd2ce67bcbf89cf2aee798c56cfb9e225e57e8c8270021210
494460a17bec58d47212c907e7e7706dc80e99b27a022558637caebc2867e574
11464f7ac40e3e5f771dfe19aee3b3d21cf526a11429038ba9de4c9d7e4bb42a
1c6c79b07e45630debe31362e4c89ffab3560c4712470f7af891bb31539d153a

Domains:

2024-aimp[.]info
2024-aimp[.]pw
2024aimp[.]info
2024aimp[.]top
2024concur[.]com
2024lexisnexis[.]com

461

a-asana[.]com
advanced-ip-scanner[.]cfd
advanced-ip-scanner[.]link
advanced-ip-scanner[.]xyz
advancedipscannerapp[.]com
aimp[.]day
aimp[.]link
aimp[.]pm
aimp[.]xyz
aimp2024[.]pw
airtables[.]net
app-trello[.]com
as-a-n4[.]com
as-an-a[.]org
as4na[.]com
asaana[.]net
asana[.]pm
asana[.]tel
asana[.]wf
asanaa[.]net
assana[.]monster
assana[.]vip
bloomberg-t[.]com
c0ncuur[.]com
c0oncur[.]com
cnn-news[.]org
concur-cloud[.]net
concur-sap[.]info
concur-sap[.]life
concur-sap[.]one
concur-sap[.]pro
concur[.]cfd
concur[.]life
concur[.]pm
concur[.]re
concur[.]skin
concur2024[.]com
concur24news[.]one
concurnews[.]one
concuur[.]com
concuur[.]net
concuur[.]org
gl-meet2024[.]com
law2024[.]info
law2024[.]top
law360[.]one
lexis-nexis[.]site
lexis2024[.]info
lexis2024[.]pro
lexisnex[.]pro
lexisnex[.]team
lexisnex[.]top
lexisnexis[.]day
lexisnexis[.]lat
lexisnexis[.]one

lexisnexis[.]pro
lexisnexis[.]top
lexisnexis2024[.]com
lexisnexises[.]net
meet-gl[.]com
meet-go[.]click
meet-go[.]day
meet-go[.]info
meet-go[.]link
meet-go[.]org
meet-goo[.]net
meet-goo[.]org
meet[.]com[.]de
meet2024[.]com
meetgo2024[.]life
meetgo2024[.]top
news-cnn[.]net
newsconcur[.]one
newsconcur2024[.]life
newsconcur2024[.]world
newsconcur24[.]one
nmap[.]re
quicken-install[.]com
sapc0ncur24[.]one
sapconcur[.]pro
sapconcur[.]top
thomsonreuter[.]info
thomsonreuter[.]pro
wal-streetjournal[.]com
wall-street-journal[.]link
webex-install[.]com
wen-airdrop[.]net
wen-airdrop[.]network
westlaw[.]top
workable[.]uk[.]com
wsj[.]pm
wsj[.]re
wsj[.]wales
wsj[.]wf
2024-7zip-10[.]shop
2024-7zip-10[.]top
2024-7zip[.]info
2024-7zip[.]pw
20247zip[.]one
7-zip[.]cfd
7-zip[.]day
7-zip[.]shop
7zip-1508[.]one
7zip-1508[.]top
7zip-2024[.]cfd
7zip-2024[.]info
7zip-2024[.]pro
7zip-archiver[.]click
7zip-archiver[.]shop
7zip-org[.]live

7zip[.]sbs
7zip10-2024[.]life
7zip10-2024[.]live
7zip10-2024[.]top
7zip1024[.]life
7zip1024[.]live
7zip1024[.]top
7zip2024[.]info
7zip2024[.]one
7zip2024[.]pro
7zip2024[.]shop
7zip2024[.]store
7zip2024[.]top
7zipx[.]site
7zlp112024[.]top
7zlp2024[.]shop
7zlp2024[.]top
h2[.]den4ik440[.]ru
seven-zip[.]click
sevenzip[.]shop
sevenzip[.]today

**********IoCs
END**********

Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Train employees to recognize fake browser updates and fake download pages. Incorporate the latest lure schemes and attack trends into training to keep awareness current. Regular training can significantly reduce the risk of user actions leading to an infection.
- Reduce the amount of sensitive data stored to limit potential exposure in case of a breach, particularly in scenarios involving double extortion attacks where attackers might threaten to leak stolen data.
- Implement strong access controls and follow the principle of least privilege, ensuring users only have the permissions necessary to perform their designated tasks.
- Limiting administrative rights can prevent ransomware from spreading across systems and causing extensive damage.

Reference: https://go.recordedfuture.com/hubfs/reports/cta-2025-0613.pdf

Note: TA-TAG: Threat Alert Threat Actor Group

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: GREEN. Limited disclosure, recipients can spread this within their community. Sources may use TLP: GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP: GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP: GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/

advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

---

advisory@nciipc.gov.in mailing list



Fwd: Advisory No: TA-MAW-2025-07-09-010: Qwizzserial Android Malware [TLP: CLEAR]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Thu, 10 Jul 2025 9:39:38 AM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Wed, 09 Jul 2025 12:31:19 +0530
Subject: Advisory No: TA-MAW-2025-07-09-010: Qwizzserial Android Malware [TLP: CLEAR]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-MAW-2025-07-09-010

Cyber Security Advisory: Qwizzserial Android Malware

This data is to be considered as TLP: CLEAR

It has been observed that a newly identified Android malware strain, known as Qwizzserial, is actively targeting users by stealing banking credentials and two-factor authentication (2FA) codes. This malware presents a significant security risk, particularly in environments where SMS-based authentication is widely employed.

Distribution Method:
Qwizzserial is primarily distributed through messaging platforms, masquerading as legitimate government-related support applications.

Capabilities:

- Requests sensitive permissions such as read SMS, make calls, and access phone state.
- Uses persistence techniques to maintain access, including bypassing battery optimization settings.
- Harvests SMS messages and applies regex patterns to extract financial and balance-related data.
- Exfiltrates collected data via HTTP POST requests to attacker-controlled infrastructure.
- Features recent updates that include code obfuscation and enhanced operational security.

**********IOC START**********

Hashes:

ea6a11a6e5da7a82bbcaca86c3d35b22f241b20f6ba5ae5e48eded99e19f6aa5
8dd5f2f406ce0d11a3c75d511b69350ba1160ed780b6b4a0f3193eb087553cca
d17cbffec701b2759707925b2ad32e15bbdead62d2be8983143daba29e1c58ff
cd0e4b2bb2f1cd2e7fbcd7846220a590900797373db37299f4e2859b1cc6d1b9
0789278eab1941ac4466ca6d043165fdb7bb333f07b2b252acb446ed2f7344da
a1c54ca63584bbf25b2f837e8a19ddb817aa1f4adfe9e9dbd630467d0b21a4a3
df8c4560449bf24f85f51ea5f99299bcdd62d821ce9ad1f6a2733a31e6206091
f29dea9aa5425877ba00d4797e0e3e32ce4e7be5a8c566cc0608e52ad6679e6c
992d2bde2fe4f4aafd6a1fa21915c78419824db52137dfdb4f801627084de300

**********IOC END**********

Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Avoid downloading apps from untrusted or unofficial sources.
- Use Android's "Google Play Protect" and enable app verification.
- Grant apps only the minimum required permissions.
- Deploy mobile security solutions to detect and block malware.
- Keep Android devices and apps up to date with the latest security patches.
- Train users to recognize phishing attempts and suspicious application behavior.

Reference: CERT-IN [CMTX-P072025156]
Note: TA-MAW: Threat Alert Malware Advisory

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: CLEAR. Recipients can spread this to the world, there is no limit on disclosure. Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

advisory@nciipc.gov.in mailing list





Fwd: Advisory No:TA-MAW-2025-07-09-008: ACR Stealer [TLP: CLEAR]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Thu, 10 Jul 2025 9:39:50 AM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Wed, 09 Jul 2025 12:16:43 +0530
Subject: Advisory No:TA-MAW-2025-07-09-008: ACR Stealer [TLP: CLEAR]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-MAW-2025-07-09-008

Cyber Security Advisory: ACR Stealer

This data is to be considered as TLP: CLEAR

It has been observed that threat actor SheldIO is distributing ACR Stealer, a sophisticated information-stealing malware, under the Malware-as-a-Service (MaaS) model. The ACR Stealer represents an advanced iteration of the GrMsk Stealer. It targets Windows systems and is designed to harvest sensitive data including credentials, browser cookies, crypto wallets and system information.

Distribution Method:

- Phishing Emails: Malicious attachments prompting macro execution.
- Cracked Software & Keygens: Popular lure for pirated software users.

- Web Injects & Fake CAPTCHAs: Delivered via compromised websites using ClearFake campaigns.
- Dead Drop Resolver (DDR): Uses online platforms to dynamically fetch Command & Control (C2) domains.

Impacts:

- Credential Theft: Access to email, social media, banking, and enterprise systems.
- Financial Fraud: Theft of crypto wallets and payment credentials.
- Identity Theft: Harvesting of PII and sensitive documents.
- Operational Disruption: Persistent infections and lateral movement.
- Data Exfiltration: Via encrypted channels and legitimate services.

TTPs (MITRE ATT&CK mapping):

- T1566.001 - Spear Phishing Attachment
- T1204 - User Execution via macros or executables
- T1064 - Scripting for payload delivery
- T1547.001 - Registry Run Keys / Startup Folder for persistence
- T1053 - Scheduled Task creation
- T1003 - Credential Dumping from browsers
- T1119 - Automated Collection of sensitive files
- T1041 - Exfiltration over C2 channels
- T1071 - Application Layer Protocol for stealthy C2
- T1483 - Domain Generation Algorithms for evasion

**********IOC
START**********
IP : Port
193[.]32[.]176[.]103:443
185[.]76[.]243[.]212:443
185[.]76[.]243[.]209:443
185[.]76[.]243[.]208:443
185[.]76[.]243[.]215:443
185[.]76[.]243[.]214:443

**********IOC
END**********
Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Enable Multi-Factor Authentication (MFA) across all accounts.
- Educate users on phishing and social engineering tactics.
- Avoid downloading cracked software or keygens.
- Apply security patches, especially for Microsoft internet shortcut files security feature bypass vulnerability (CVE-2024-21412) exploited by ACR Stealer.
- Monitor Google Drive API activity for anomalies.
- Deploy advanced endpoint protection and behavior-based detection.
- Implement network monitoring to detect unusual Command & Control (C2) traffic.

Reference: CERT-IN [CMTX-P072025775]
Note: TA-MAW: Threat Alert Malware Advisory

470

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: CLEAR. Recipients can spread this to the world, there is no limit on disclosure. Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

advisory@nciipc.gov.in mailing list



Fwd : Advisory No: TA-MAW-2025-07-09-009: XtremeRAT [TLP: CLEAR]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Thu, 10 Jul 2025 9:40:02 AM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Wed, 09 Jul 2025 12:24:28 +0530
Subject: Advisory No: TA-MAW-2025-07-09-009: XtremeRAT [TLP: CLEAR]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-MAW-2025-07-09-009

Cyber Security Advisory: XtremeRAT

This data is to be considered as TLP: CLEAR

It has been observed that XtremeRAT, a publicly available Remote Access Trojan (RAT), has undergone numerous updates and served as the foundation for the development of several other RAT tools. It is primarily distributed through medium-scale spam campaigns. Upon successful execution, XtremeRAT attempts to establish a backdoor in the target system to enable communication with its Command and Control (C2) infrastructure.

Impact: System Compromise: Remote attackers can gain control of vulnerable systems.

Capabilities:

- Target interaction via remote shell.
- Transfer and execute files.
- Manipulate processes and services.
- Alter registry entries.
- Capture desktop images.
- Record from connected devices, such as webcams or mice, with the recorded data written to an RC4 encrypted log file.

**********IOC
START**********
IP : Port
118[.]107[.]244[.]105:10001
92[.]205[.]165[.]168:10001
173[.]234[.]30[.]74:10001
223[.]247[.]220[.]26:10001

**********IOC
END**********
Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- A comprehensive training program is in place to educate users on identifying and avoiding unsolicited emails, including the risks of opening attachments or clicking unknown links.
- Install and regularly update antivirus software.
- Install Updates and Patches regularly.
- Conduct regular backup practices and keep those backups offline or on a separate network.
- Implement Multi-Factor Authentication (MFA).
- All day to day computer activities such as email and internet are performed using non-administrative accounts.
- Enforced password policies require strong credentials, and users are discouraged from reusing passwords across different systems.
- Network, proxy and firewall logs should be monitored for suspicious activity.
- User accounts accessed from infected machines should be reset on a clean computer.

Reference: CERT-IN [CMTX-P072025196]
Note: TA-MAW: Threat Alert Malware Advisory

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: CLEAR. Recipients can spread this to the world, there is no limit on disclosure. Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction
Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

advisory@nciipc.gov.in mailing list



Fwd: Advisory No: TA-MAW-2025-07-09-007: MooBot Malware [TLP: CLEAR]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Thu, 10 Jul 2025 9:40:15 AM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Wed, 09 Jul 2025 12:12:19 +0530
Subject: Advisory No: TA-MAW-2025-07-09-007: MooBot Malware [TLP: CLEAR]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-MAW-2025-07-09-007

Cyber Security Advisory: MooBot Malware

This data is to be considered as TLP: CLEAR

It has been observed that MooBot, a Mirai-family malware variant is targeting D-Link Linux-based networking devices, exploiting multiple remote execution flaws to hijack routers for malicious use.

Capabilities:

- Connects to its C2 infrastructure
- Sends status updates to its command-and-control server
- Listens for commands to launch DDoS attacks, targeting specific IPs and ports
- Infected devices are fully controlled, enabling mass-scale attacks

Impact: Attack complexity is low, yet the impact is high, enabling wide-scale remote compromise of Commercial Off-The-Shelf devices.

**********IOC
START**********
IP : Port
195[.]26[.]230[.]140:80
196[.]251[.]116[.]143:80
157[.]185[.]143[.]171:18086

**********IOC
END**********
Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Immediate firmware/OS updates or device replacement for all D-Link devices.
- Monitor network traffic for unusual outbound connections to known C2 patterns.
- Deploy IoT-focused intrusion prevention tools and enforce strong device credential policies.

Reference: CERT-IN [CMTX-P072025206]
Note: TA-MAW: Threat Alert Malware Advisory

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: CLEAR. Recipients can spread this to the world, there is no limit on disclosure. Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction

Disclaimer:
The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

advisory@nciipc.gov.in mailing list





Fwd: Advisory No: TA-MAW-2025-07-09-006: GIFTEDCROOK Infostealer [TLP: CLEAR]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Thu, 10 Jul 2025 9:40:30 AM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Wed, 09 Jul 2025 12:07:17 +0530
Subject: Advisory No: TA-MAW-2025-07-09-006: GIFTEDCROOK Infostealer [TLP: CLEAR]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-MAW-2025-07-09-006

Cyber Security Advisory: GIFTEDCROOK Infostealer

This data is to be considered as TLP: CLEAR

It has been observed that GIFTEDCROOK, a malware tool developed by the cyber-espionage group UAC-0226, has evolved from a simple browser data stealer to a sophisticated intelligence-gathering tool. It shares infrastructure with campaigns utilizing NetSupport RAT, further demonstrating its advanced capabilities. The malware's use of credible, themed phishing emails and its real-time alignment with geopolitical events underscore a strategic approach to espionage. Notably, the primary sectors targeted by GIFTEDCROOK include government and military institutions.

Delivery Method: Spear-phishing emails with military-themed lures.

Exfiltration Method: Files encrypted and compressed before exfiltration via Telegram bot channels.

MITRE ATTACK IDENTIFIERS:

- T1204.002 - Malicious File
- T1566.002- Spearphishing Link
- T1555 - Credentials from Password Stores
- T1005 - Data from Local System
- T1041- Exfiltration Over C2 Channel

**********IOC START**********

Hashes:

4e61215d2f5323942ef2cf737d6cb7c2755820796325ceef4e4b5d7e7aef2208
1974709f9af31380f055f86040ef90c71c68ceb2e14825509babf902b50a1a4b
ca2585acb9e37f5f46705f8f00d69453bfce7dc9327af0325a7ad8a88bf549a7
399c0881230f6309f1fead5dae33021a40ae2a4c37edac1c24c9b4e1a0e630f9
c2e920944d994ba28bc9e159491a89d83e305e63fafc4a4e25433db63800d5fa
f6b03fa3ea7fd2c4490af19b3331f7ad384640083757a3cede320ca54c7b0999
a7a2895e4c10866967eff3ec719a2f697c859888af6482f6697e90042cb5d5b2
a6dd44c4b7a9785525e7f487c064995dc5f33522dad8252d8637f6a6deef3013
b9d508d12d2b758091fb596fa8b8b4a1c638b7b8c11e08a1058d49673f93147d

URLs:

hxxps://api[.]telegram[.]org/bot7806388607:AAFb6nCE21n6YmK6-bJA6IrcLTLfhlwQ254/sendDocument
hxxps://api[.]telegram[.]org/bot7726014631:AAFe9jhCMsSZ2bL7ck35PP30TwN6Gc3nzG8/sendDocument

**********IOC END**********

Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Educate employees on phishing detection.
- Block spoofed and malicious emails.
- Detect and contain malware activity.
- Investigate anomalous outbound Telegram communications.

***Reference*:** CERT-IN [CMTX-P072025106]
Note: TA-MAW: Threat Alert Malware Advisory

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: CLEAR. Recipients can spread this to the world, there is no limit on disclosure. Subject to standard copyright rules, TLP: CLEAR information may be shared without restriction

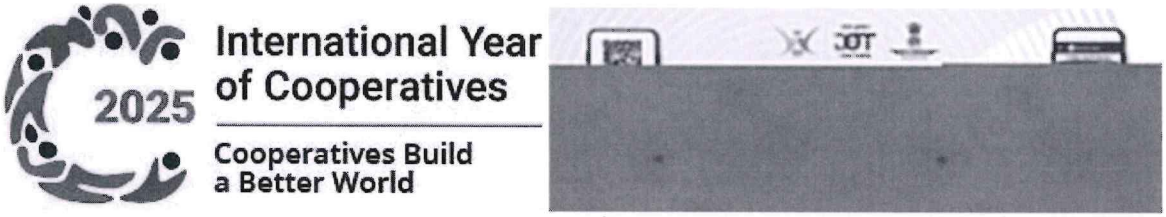
Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will

not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

---

advisory@nciipc.gov.in mailing list



Fwd: Advisory No: VA-2025-07-07-006: Active Exploitation of Vulnerabilities in Ivanti Endpoint Manager Mobile [TLP: GREEN]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Mon, 07 Jul 2025 4:05:25 PM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Mon, 07 Jul 2025 15:30:13 +0530
Subject: Advisory No: VA-2025-07-07-006: Active Exploitation of Vulnerabilities in Ivanti Endpoint Manager Mobile [TLP: GREEN]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: VA-2025-07-07-006

Cyber Security Advisory: Active Exploitation of Vulnerabilities in Ivanti Endpoint Manager Mobile

This data is to be considered as **TLP: GREEN**

It has been observed that threat actors are exploiting the authentication bypass vulnerability (CVE-2025-4427) and Remote Code Execution (RCE) vulnerability (CVE-2025-4428) in Ivanti Endpoint Manager Mobile (EPMM). These vulnerabilities, when exploited in combination, enable unauthenticated (RCE) in exposed systems. Active exploitation of this vulnerability-chain has been observed, targeting internet-facing EPMM deployments across a range of sectors, including healthcare, telecommunications, aviation, municipal government, finance and defense.

Successful exploitation is carried out by a threat group with advanced knowledge of EPMM's internal architecture, repurposing legitimate system components for covert data exfiltration. This includes the extraction of large volumes of Personally Identifiable Information (PII), authentication credentials and other sensitive data, which are then used for lateral movement within compromised networks. Given EPMM's role in managing and configuring enterprise mobile devices, the exploitation could allow threat actors to remotely access, manipulate, or compromise thousands of managed devices within an organisation.

Affected Products: Ivanti Endpoint Manager Mobile (EPMM) version 12.5.0.0 and earlier.

Payloads and Persistence:

- KrustyLoader Malware: After gaining initial access, the attackers deploy KrustyLoader, a malicious payload, which is responsible for establishing long-term persistence on the compromised system. The malware retrieves additional payloads and performs encryption, hiding the true nature of its operations.
- Encrypted Backdoor: The KrustyLoader decrypts and loads a second-stage payload, often an encrypted version of a backdoor, directly into system memory. This process enables covert, continuous access for attackers even after patching efforts.

Impact:

- Persistent Access: Attackers can maintain access even after the initial vulnerability is patched.
- Data Theft: Sensitive operational data, including authentication credentials, personal data, and internal network configurations, is exfiltrated.
- Network Exploitation: Attackers use tools to expand their control across the network, moving laterally to gain access to additional systems.

**********IOC START**********

Hashes:

44c4a0d1826369993d1a2c4fcc00a86bf45723342cfd9f3a8b44b673eee6733a
7a4e0eb5fbab9709c8f42beb322a5dfefbc4ec5f914938a8862f8e26a31d30a5
f34db4ea8ec3c2cbe53fde3d73229ccaa2a9e7168cd96d9a49bf89adef5ab47c
150ccd3b24a1b40630e46300100a3f810aa7a6badeb6806b59ed6ba7bafb7b21
29ae4fa86329bf6d0955020319b618d4c183d433830187b80979d392bf159768
64764ffe4b1e4fc5b9fe27b513e02f0392f659c4e033d23a4ba7a3b7f20c6d30
b422645db18e95aa0b4daaf5277417b73322bed306f42385ecfd6d49be26bfab

Domains:

openrbf.s3.amazonaws[.]com
tnegadge.s3.amazonaws[.]com
fconnect.s3.amazonaws[.]com
trkbucket.s3.amazonaws[.]com
the-mentor.s3.amazonaws[.]com
tkshopqd.s3.amazonaws[.]com
ns1.cybertunnel[.]run

URLs:

hxxp://abbeglasses.s3[.]amazonaws[.]com/dSn9tM
hxxps://dpaste[.]com/9MQEJ6VYR.txt

IPs:

103.244.88[.]125
27.25.148[.]183
146.70.87[.]67:45020

481

124.223.202[.]90

**********IOC
END**********

Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Organizations are strongly advised to apply Ivanti released patches addressing both vulnerabilities. Ivanti has released updates for Endpoint Manager Mobile (EPMM). Organisations should install one of the fixed versions 11.12.0.5, 12.3.0.2, 12.4.0.2 or 12.5.0.1.

Note: VA: Vulnerability Advisory

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: GREEN. Limited disclosure, recipients can spread this within their community. Sources may use TLP: GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP: GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP: GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

advisory@nciipc.gov.in mailing list





Fwd: Advisory No: VA-2025-07-07-005: Critical Vulnerabilities in Multiple Products [TLP: CLEAR]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Mon, 07 Jul 2025 4:05:33 PM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Mon, 07 Jul 2025 15:17:40 +0530
Subject: Advisory No: VA-2025-07-07-005: Critical Vulnerabilities in Multiple Products [TLP: CLEAR]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: VA-2025-07-07-005

Cyber Security Advisory: Critical Vulnerabilities in Multiple Products

This data is to be considered as TLP: CLEAR

Critical Vulnerability in Craft CMS
A critical Remote Code Execution (RCE) vulnerability was discovered in Craft CMS, a user-friendly CMS for creating custom digital experiences on the web and beyond. The RCE vulnerability was assigned the CVE ID CVE-2025-32432 with a CVSS score of 10.0. The affected versions are Craft starting from version 3.0.0-RC1 to before 3.9.15, 4.0.0-RC1 to before 4.14.15, and 5.0.0-RC1 to before 5.6.17. Craft has released fixed CMS versions: 3.9.15, 4.14.15 and 5.6.17 to resolve the RCE vulnerability.
References:
https://nvd.nist.gov/vuln/detail/CVE-2025-32432
https://sensepost.com/blog/2025/investigating-an-in-the-wild-campaign-using-rce-in-craftcms/

Critical Vulnerabilities in Siemens
Critical arbitrary code execution (CVE-2025-26389) and SQL injection (CVE-2025-26390) vulnerabilities

have been discovered in Siemens OZW Web Servers. The CVE ID CVE-2025-26389 has a CVSS score of 10.0 and CVE-2025-26390 has a CVSS score of 9.8. The affected versions are Siemens OZW672 and OZW772 Web Server. Siemens has released new versions of the affected products and recommends updating to the latest versions.
Reference: https://cert-portal.siemens.com/productcert/html/ssa-047424.html

Multiple Vulnerabilities in Ivanti
Critical authentication bypass (CVE-2025-4427) and Remote Code Execution (RCE) (CVE-2025-4428) vulnerabilities have been discovered in Ivanti Endpoint Manager Mobile (EPMM) version 12.5.0.0 and earlier. When chained together, these vulnerabilities can allow unauthenticated RCE on vulnerable systems. Ivanti has released updates for Endpoint Manager Mobile (EPMM). Customers should install one of the fixed versions 11.12.0.5, 12.3.0.2, 12.4.0.2 or 12.5.0.1.
Reference: https://www.fortiguard.com/threat-signal-report/6104/ivanti-epmm-zero-day-vulnerabilities

Critical Vulnerability in Erlang/OTP SSH
A critical vulnerability has been discovered in the Erlang/Open Telecom Platform (OTP) SSH implementation that allows an attacker to perform unauthenticated Remote Code Execution (RCE). Successful exploitation of SSH protocol message handling could allow unauthorized access to affected systems and execute arbitrary commands without valid credentials. This vulnerability has been assigned the CVE ID CVE-2025-32433 with an estimated CVSSv3 score of 10.0. Users are advised to update to the latest available Erlang/OTP release. The fixed versions are OTP-27.3.3 (for OTP-27), OTP-26.2.5.11 (for OTP-26) and OTP-25.3.2.20 (for OTP-25) to mitigate this issue.
References:
https://www.openwall.com/lists/oss-security/2025/04/16/2
https://github.com/erlang/otp/security/advisories/GHSA-37cp-fgq5-7wc2

Critical Vulnerability in Commvault Command Center
A critical path traversal vulnerability has been discovered in Commvault's Command Center that allows remote attackers to execute arbitrary code without the need for authentication and exposes the Command Center environment to full compromise. This vulnerability has been assigned the CVE ID CVE-2025-34028 and is given a maximum CVSS score of 10.0. By exploiting this flaw, an attacker can gain unauthorised access, potentially compromising sensitive data and disrupting services. The vulnerability was present only in the 11.38 Innovation Release of the Command Center and does not affect later versions. Commvault has issued a fix for this vulnerability in the subsequent Innovation Update releases, which addresses the vulnerability and mitigates the risk of exploitation.
Reference: https://documentation.commvault.com/securityadvisories/CV_2025_04_1.html

Vulnerability in Microsoft's OneDrive File Picker
Oasis Security's research team has identified a critical vulnerability in Microsoft's OneDrive File Picker. This vulnerability in Microsoft's OneDrive File Picker allows websites to access a user's entire OneDrive content, rather than just the specific files selected for upload via OneDrive File Picker. The issue stems from the File Picker requesting broad read permissions due to the lack of fine-grained OAuth scopes in OneDrive. As a result, applications integrated with OneDrive—such as ChatGPT, Slack, Trello, and ClickUp—are potentially impacted. The OAuth consent screen presented to users is vague, failing to clearly communicate the extent of access being granted. This opens users up to significant security risks, especially when they believe they're only sharing one file but unknowingly authorise access to their full drive. Further compounding the risk, OAuth tokens are often stored insecurely—in plain text within browser session storage—making them vulnerable to exploitation. Microsoft has acknowledged the issue but has yet to release a fix. Until a secure resolution is provided, developers and organisations are advised to consider disabling OneDrive file uploads via OAuth to protect user data from unauthorized access and potential misuse.
References:
https://www.oasis.security/blog/onedrive-file-picker-security-flaw-oasis-research
https://pages.oasis.security/rs/106-PZV-596/images/onedrive-file-access-warning.pdf?version=0
https://thehackernews.com/2025/05/microsoft-onedrive-file-picker-flaw.html
https://learn.microsoft.com/en-us/onedrive/developer/controls/file-pickers/?view=odsp-graph-online

Note: *VA: Vulnerability Advisory*

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: CLEAR. Recipients can spread this to the world, there is no limit on disclosure. Subject to standard copyright rules, TLP: CLEAR information may be shared without

restriction.

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

---

advisory@nciipc.gov.in mailing list



Fwd: Advisory No: TA-APT-2025-07-07-001: APT36 Campaign [TLP:GREEN]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Mon, 07 Jul 2025 5:36:35 PM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Mon, 07 Jul 2025 17:01:18 +0530
Subject: Advisory No: TA-APT-2025-07-07-001: APT36 Campaign [TLP:GREEN]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-APT-2025-07-07-001

Cyber Security Advisory: APT36 Campaign

This data is to be considered as **TLP: GREEN**

It has been observed that APT36, also known as Transparent Tribe, has expanded its tactics to target Linux-based environments, specifically BOSS Linux, a distribution widely used by government agencies. For initial access, adversaries send phishing emails containing a ZIP file that holds a malicious [.]desktop file, which acts as a Linux shortcut. Upon execution, this file triggers a dual-action mechanism, not only downloading and opening a legitimate PowerPoint file to appear authentic, but also silently downloading & executing a malicious ELF binary in the background.

This ELF binary is the primary payload, designed to compromise the system and enable unauthorised access. The malicious binary client.elf, allowing it to run either silently in the background or interactively through a visible terminal. This flexibility enables the attacker to operate the malware covertly or observe its behavior directly, depending on their objective. The malware gathers system hostname, CPU, and RAM details to profile the victim's machine and tailor its malicious actions. The malware leverages main.loadConfig to retrieve operational settings, including Command & Control (C2) server details. This

multi-stage approach is aimed at bypassing user suspicion and evading traditional security measures, allowing the attackers to maintain persistent access to sensitive systems. The use of Linux-specific malware indicates an evolution in APT36's capabilities, posing an increasing threat to critical government and defense infrastructure.

MITRE ATT&CK Framework:

- Initial Access
  - T1566 Phishing
  - T1566.001 Spear phishing Attachment
- Execution
  - T1064 Scripting
- Persistence
  - T1543 Create or Modify System Process
  - T1543.003 Systemd Service
- Privilege Escalation
  - T1543 Create or Modify System Process
  - T1543.002 Systemd Service
- Defense Evasion
  - T1036 Masquerading
  - T1064 Scripting
  - T1564 Hide Artifacts
  - T1564.001 Hidden Files and Directories
- Discovery
  - T1518 Software Discovery
  - T1518.001 Security Software Discovery
- Command and control
  - T1071 Application Layer Protocol
  - T1095 Non-Application Layer Protocol
  - T1105 Ingress Tool Transfer
  - T1571 Non-Standard Port

**********IOC
START**********
Domains:
sorlastore[.]com
modgovin[.]onthewifi[.]com

URLs:
hxxp://169[.]254[.]169[.]254/latest/meta-data/ami-id
hxxps://govin[.]sorlastore[.]com/uploads/Cyber-Security-Advisory[.]pptx
hxxps://govin[.]sorlastore[.]com/uploads/BOSS[.]elf

Hashes:
608fff2cd4b727799be762b95d497059a202991eb3401a55438071421b9b5e7a
ace379265be7f848d512b27d6ca95e43cef46a81dc15d1ad92ec6f494eed42ab
e528799a29e9048c1e71b78223311cad2699d035a731d1a6664fc8ddd0642064
167b387005d6d2a55ad282273c58d1786a2ee0fa3e7e0cb361d4d61d8618ee5f

IPs:
169[.]254[.]169[.]254
101[.]99[.]92[.]182

**********IOC
END**********
Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Implement advanced email filtering to detect and block phishing attempts, especially those containing .desktop files, ZIP archives and executable content.
- Disable execution of email attachments by default, unless explicitly verified.

487

- Conduct regular cybersecurity awareness training focused on phishing tactics, social engineering, and suspicious file types (e.g., .desktop, .elf, .pptx from unknown sources).
- Encourage a zero-trust mindset, where users are trained not to open unsolicited attachments or click on unknown links, especially in government and defense environments.
- Restrict execution permissions on directories like /tmp to limit the ability of malware to execute from writable paths.
- Disable or limit support for .desktop files in email clients and file managers unless they come from trusted sources.
- Implement application whitelisting to prevent unauthorized applications (such as unknown ELF binaries) from running.
- Deploy EDR (Endpoint Detection and Response) tools capable of detecting Linux threats, unauthorized process execution, and unusual network behavior.
- Monitor outbound traffic for unusual or unauthorized connections to suspicious domains (e.g., sorlastore.com) that may indicate malware beaconing or payload delivery.
- Use network segmentation to limit the spread of malware within critical systems and infrastructure.
- Ensure BOSS Linux systems and all open-source applications (like LibreOffice, curl, etc.) are up to date with the latest security patches to reduce exploitation vectors.
- Use behavior-based detection rules to flag suspicious use of tools like curl, chmod, and nohup, especially when chained together in scripts or .desktop files.
- Block execution of unknown binaries downloaded via scripts unless verified and signed by the organization.

Reference: https://www.cyfirma.com/research/phishing-attack-deploying-malware-on-indian-defense-boss-linux/

Note: TA-APT: Threat Alert - Advanced Persistent Threat

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website:www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: GREEN. Limited disclosure, recipients can spread this within their community. Sources may use TLP: GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP: GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP: GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.

Disclaimer:
The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

advisory@nciipc.gov.in mailing list



Fwd: Advisory No: TA-MAW-2025-07-08-005: Threat Actors Developing Cracking Websites for Stealer Malware Distribution [TLP: GREEN]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Wed, 09 Jul 2025 9:23:07 AM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/SIr

Pl do the needful

O/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Tue, 08 Jul 2025 16:48:20 +0530
Subject: Advisory No: TA-MAW-2025-07-08-005: Threat Actors Developing Cracking Websites for Stealer Malware Distribution [TLP: GREEN]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-MAW-2025-07-08-005

Cyber Security Advisory: Threat Actors Developing Cracking Websites for Stealer Malware Distribution

This data is to be considered as **TLP: GREEN**

It has been observed that threat actors are leveraging a pay-per-install model to distribute stealer malware via cracking websites. Adversaries, skilled in web development and online advertising, build and maintain malicious websites that offer cracked software. The compromised credentials from these websites are sold or traded on cybercrime forums, enabling further attacks like ransomware or espionage. Adversaries often use SEO and paid advertising to promote their sites, making it harder to trace. The infrastructure behind this operation is spread across multiple domains and hosting services.

**********IOC START**********

Domains:

Pcserialkey[.]com
Cracxfree[.]com
Vlsoft[.]net
Pcproductkey[.]net
Vsthomes[.]com
Sadeempc[.]com
Crackedpc[.]net
Apxsoftwares[.]com
Fullcrackedpc[.]com
Xproductkey[.]com
Keygenned[.]com
Downloadcracker[.]com
Ratondownload[.]net
Crackbay[.]org
Filehorsed[.]com
Activatedcrack[.]com
Goldenapk[.]com
Pcmage[.]co
Azcrack[.]org
Hmcrack[.]org
Axcrack[.]org
A2zpc[.]org
Activatorkey[.]com
Licenselink[.]info
Vst4plugins[.]com
Samipc[.]org
Azcracked[.]com
Citycrack[.]com
Licensedkey[.]co
Cracksvst[.]com
Filehippos[.]co
Docrack[.]org
Crack4pro[.]com
Crackhome[.]net
Spsoftwares[.]com
Softwarezstore[.]com
Prosoftz[.]com
Devcrack[.]org
Crackedactivator[.]com
Crackedexe[.]com
Piratesfile[.]org
Cracklicense[.]net
Crackzip[.]net
Allcracksoft[.]org
Suripc[.]com
Fullcrackedpc[.]org
Installlink[.]org
Cracked4pc[.]info
Pcmaccrack[.]com
Cracklink[.]info
Igetintopc[.]info
Crsoftz[.]com
Crackwin7[.]com
Encrack[.]net

94fbr[.]org
Click4pc[.]com
Procrackedpc[.]com
Keykeygen[.]com
Pcsoftz[.]net
Filepuma[.]org
Softncrack[.]com
Freekeygen[.]net
Prosvst[.]com
Freeactivationkeys[.]com
Filecrk[.]com
Up2pc[.]org
Softspedia[.]org
Softwarezpro[.]info
Crack4box[.]com
Zainabpc[.]com
Crackme[.]info
Freeprosoft[.]org
Crackdownloader[.]net
Corecrack[.]org
Allpcsoftwares[.]info
Activatorhax[.]com
Mahcrack[.]com
Serialkeygenpro[.]com
Allpcsoft[.]net
Artcrack[.]org
Softwarecrack[.]org
Sehrpc[.]com
Ahcracks[.]com
Procrack[.]co
Crackedsofts[.]info
Crackedloader[.]com
Filehipo[.]co
Crackproz[.]org
Turkycrack[.]com
Crackmax[.]org
Hdlicense[.]org
Kmspicoproductkey[.]com
Crackclue[.]com
Gocrack[.]net
Momopc[.]org
Portablecrack[.]co
Vstfine[.]com
Beecrack[.]com
Activatorspatch[.]com
Plugtorrent[.]com
Parrotpc[.]org
Ecrack[.]org
Vstmac[.]com
Descargarpc[.]org
Softwaregurucrack[.]com
Wincrack[.]org
Mzcrack[.]com
Crackactivation[.]info
Cracksumo[.]net

Freeprosoftz[.]org
Fullcrackerz[.]co
Provst[.]net
Fullkeys[.]net
Cractivator[.]com
Crackpaper[.]org
Freeserialkey[.]net
Crackpatch[.]info
Cracked4soft[.]com
Crackedios[.]com
Hamapc[.]com
Kalicrack[.]org
Crack4tech[.]net
Fullfreecracked[.]com
Filespcdownload[.]com
Getprocrack[.]org
Cracked4free[.]com
Freeproductkey[.]net
Crackedrules[.]com
Startcrack[.]org
Vstcomplex[.]com
Vstdownloader[.]com
Freesoftpc[.]net
Crackserialkey[.]net
Vstmacdownload[.]com
Free4pc[.]info
Activatorproductkey[.]com
Lulucrack[.]com
Realproductkeys[.]com
Malacrack[.]org
Crackmust[.]com
Activationcrack[.]com
9to5mac[.]org
Freesoftpc[.]org
Crackbank[.]org
Wazusoft[.]net
Proactivator[.]org
Downloadscrack[.]com
Extrack[.]org
Cocrack[.]net
Cracknew[.]info
Systemcrack[.]net
Vstbank[.]net
Allpc[.]org
Cracklayer[.]com
Vstpromax[.]com
Crackshome[.]org
Activationkeyspro[.]org
Fullversionsoft[.]info
Crackskit[.]net
Serialfull[.]info
Vstlove[.]com
Softwaresdaily[.]com
Gurucrack[.]org
Crack2dl[.]com

Activationskey[.]net
Fbr94[.]net
Filehorse[.]info
Crackfullpatch[.]com
Vstlicense[.]com
Crackxworld[.]com
Pcfile[.]org
Crackedfine[.]net
Downloadspatch[.]com
Licenselee[.]com
Crackkeys4u[.]com
Profreecracks[.]com
Kuyhaa[.]co
Iactivationkeys[.]com
Patchkey[.]net
Pcvstcrack[.]com
Chathacrack[.]com
Cloudcracked[.]com
Idmcrackeys[.]org
Tech-softwares[.]com
Crackdaily[.]net
Getintopcfree[.]net
Filescrack[.]com
Crackjin[.]net
plugvst[.]com
crackword[.]org
crackfix[.]org
zamilcrack[.]com
jincrack[.]com
freemacos[.]com
procrackerez[.]com
lulupc[.]net
ayeshapc[.]net
crackedx[.]net
crackkeygen[.]net
ganjiswag[.]net
fullversionpro[.]net
hacrack[.]com
installlink[.]net
securecrack[.]net
softnkey[.]net
pcproductkeys[.]org
soft4mac[.]org
vstmac[.]org
vstlicensekey[.]com
extrack[.]net
pcsoftnew[.]net
procrackerz[.]net
vstmac[.]net
fullgetpc[.]com
crack-vst[.]com
mahapc[.]net
procrackerez[.]net
vstprocracker[.]com
zubicrack[.]com

shezacrack[.]com
sdcrack[.]com
prdownloader[.]com
seriallink[.]org
activecrack[.]org
ashcrack[.]com
vstapps[.]net
vstsoft[.]net
vstmix[.]com
vstgurucrack[.]com
alghazalimodelschool[.]com
vstcracked[.]org
ayeshapc[.]org
plugcracked[.]org
vstmafia[.]org
pcsoftsfull[.]org
sampc[.]info
plugcrack[.]net
vstsetup[.]net
azharsoft[.]com
piratcrack[.]com
softwaresideas[.]com
samsoftz[.]com
pcsoftz[.]org
softserial[.]org
leecrack[.]com
kingcrack[.]org
softwaresguru[.]org
plugcrack[.]org
abdullahpc[.]org
cracknote[.]net
vstmafia[.]net
vstsoftware[.]net
crackdudu[.]com
freecrackerz[.]org
piratecrack[.]org
getprocrack[.]net
joincrack[.]net
softwarelink[.]net
optimalcrack[.]com
vstjin[.]com
pesktop[.]net
procrackz[.]net
productcrack[.]net
cracklee[.]net
vstforest[.]net
vstworking[.]net
soft4mac[.]net
stcrack[.]net
crackspro[.]org
starcrack[.]org
procrackz[.]org
mustcrack[.]com
crackactivater[.]com
softwarelee[.]org

prodownloader[.]org
crackdisk[.]org
softwarespro[.]org
thiscrack[.]net
vstcyberpc[.]com
vstpincrack[.]com
crackfue[.]com
crackpatch[.]net
crackmap[.]net
crackex[.]net
vstserial[.]com
thesecrack[.]net
vstpirate[.]net
zippycrack[.]net
crackapps[.]org
iamactivator[.]org
crackking[.]org
softwarepatch[.]net
serialsoft[.]net
thatcrack[.]net
vstcracker[.]com
andicrack[.]com
topcracksofts[.]com
mailcrack[.]net
crackboss[.]net
crackhouses[.]net
keygencrack[.]org
cyberspc[.]org
vstpro[.]org
smartcrack[.]org
quickideas[.]org
vstcrackpro[.]net

**********IOC
END**********

Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Regularly train employees to recognize phishing attempts, especially those involving malicious attachments or suspicious links. Conduct internal phishing tests to assess and improve employee awareness.
- Don't download cracked software and only install programs and updates from official sources.
- Use advanced email security gateways to detect and block phishing emails, particularly those containing malicious attachments or links.
- Enable Multi-Factor Authentication (MFA) for browser-related accounts to mitigate credential theft.
- Set up network monitoring to identify unusual or unauthorized outbound connections.

Reference: https://www.intrinsec.com/pakistani-freelancers-building-cracking-websites-for-stealer-delivery/

Note: TA-MAW: Threat Alert Malware Advisory

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067

Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: GREEN. Limited disclosure, recipients can spread this within their community. Sources may use TLP: GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP: GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP: GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

---

advisory@nciipc.gov.in mailing list





Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Cyber Security Advisory received From the National Critical Information Infrastructure Protection Centre (NCIIPC) reg.

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Wed, Dec 17, 2025 at 3:16 PM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **DDA AIIMS PATNA** <dda@aiimspatna.org>
Date: Mon, Aug 11, 2025 at 7:32 PM
Subject: Fwd: Cyber Security Advisory received From the National Critical Information Infrastructure Protection Centre (NCIIPC) reg.
To: Amit Kumar Sinha <amit.sinha@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **mn mishra** <mnmishra.mohfw@gmail.com>
Date: Mon, 11 Aug 2025, 18:02
Subject: Fwd: Cyber Security Advisory received From the National Critical Information Infrastructure Protection Centre (NCIIPC) reg.
To: <dda@aiimsdeoghar.edu.in>, DDA AIIMS Jodhpur <dda@aiimsjodhpur.edu.in>, DDA AIIMS Bhopal <dydir@aiimsbhopal.edu.in>, <ddamadurai1189@gmail.com>, Deputy Director Administration <dda@aiimsbhubaneswar.edu.in>, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Rishikesh <dda@aiimsrishikesh.edu.in>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, <ddaaiimsjammu@gmail.com>, ddaaiimsbilaspur <ddaaiimsbilaspur@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, <dda@aiimsnagpur.edu.in>, Dy Director Administration AIIMS, Raebareli <ddaaiimsrbl@gmail.com>, Recruitment Cell AIIMS, Bathinda <recruitmentaiimsbathinda@gmail.com>, <ciso@aiimsraipur.edu.in>, <ciso@aiimskalyani.edu.in>, <anandchellappan@aiimsnagpur.edu.in>, <shivam.tsg@aiimsbhopal.edu.in>, <head.it@aiimsjammu.edu.in>, <rohit.bio@aiimsbibinagar.edu.in>, <drraje.path@aiimsmadurai.edu.in>, <drmohanraj@aiimsgorakhpur.edu.in>, <drabhyuday@aiimspatna.edu.in>, <raj.sharma@aiimsbhubaneswar.edu.in>, <Goyal.tarun@aiimsbathinda.edu.in>, AIIMS Gorakhpur <itcellaiimsgkp@gmail.com>, <draksharphc@gmail.com>, <itincharge@aiimsrishikesh.edu.in>, <aao@aiimsdeoghar.edu.in>, <mundraa@aiimsjodhpur.edu.in>, <debboruah@aiimsguwahati.ac.in>
Cc: RaviKumar RaviKumar <ravi.kumar89@gov.in>, dharmenderkumar14 <dharmender.kumar14@gov.in>, ShriRajKumar Under Secretary <raj.kumar28@nic.in>, <arvind.thakur@nic.in>

Dear Madam/Sir,
As per trailing mail, kindly take necessary action please.

--
regards,
Er.M.N.Mishra,
PMSSY,MoHFW
Mob: 7982125857
---------- Forwarded message ---------
From: **Shri Raj Kumar Deputy Secretary** <raj.kumar28@nic.in>
Date: Mon, Aug 11, 2025 at 10:03 AM
Subject: Fwd: Cyber Security Advisory received From the National Critical Information Infrastructure Protection Centre (NCIIPC) reg.
To: Dharmendra Kumar <dharmender.kumar14@gov.in>, Ravi Kumar <ravi.kumar89@gov.in>, SUBHANSHU KUMAR <subhanshu.kumar@gov.in>, **mnmishra.mohfw** <mnmishra.mohfw@gmail.com>

Deputy Secretary
PMSSY-I/ SNA
23063178

========== Forwarded message ==========
From: eHealth Section <telmed-mohfw@gov.in>
To: "Jaideep Kumar Mishra"<asfa-mhfw@nic.in>, "Roli Singh"<asfr-mohfw@gov.in>, "Ms. Roli Singh"<ash-mohfw@nic.in>, "Ms VHekali Zhimomi"<zhimomiv@ias.nic.in>, "oo.asphp Singh"<oo.asphp-mohfw@gov.in>, "Aradhana Patnaik"<asmd-mohfw@nic.in>, "Manashvi Kumar"<jstraining-mohfw@gov.in>, "ELANGBAM ROBERT SINGH"<robert.elangbam@gov.in>, "Indrani Kaushal"<ea-mohfw@gov.in>, "gulam mustafa" <gulam.mustafa@nic.in>, "JS ME"<js.me-mohfw@nic.in>, "ANKITA MISHRA BUNDELA"<js-pmssy-mohfw@gov.in>, "Nikhil Gajraj"<nikhil.g@ias.nic.in>, "Vijay Nehra"<js-proc-mohfw@gov.in>, "Saurabh Jain"<js.policy-mohfw@gov.in>, "Vandana Jain"<vandana.jain@nic.in>, "Meera Srivastava"<jsrch-mohfw@gov.in>, "Vijay Sinha" <sinha.vijay@nic.in>, "Indrani Kaushal"<ea-mohfw@nic.in>, "Pradeep Khasnobis"<pradeep.khasnobis@gov.in>, "Rakesh Kumar Maurya"<rakesh.maurya@gov.in>, "Narendra Oza"<nk.oza@gov.in>, "KIRAN KARLAPU" <kiran.karlapu@gov.in>, "ROLI KHARE"<roli.khare@gov.in>, "Harsh Mangla"<harsh.mangla@ias.nic.in>, "SAROJ KUMAR"<saroj.kumar@nic.in>, "Sachin Kumar"<sachin.k@nic.in>, "SUSHIL Gahlaut"<sp.gahlaut@nic.in>, "Kumar Rahul"<kumar.rahul@nic.in>, "Gs Chitra"<gs.chitra@nic.in>, "Phool Prasad"<prasad-upsc@gov.in>, "Govind Kumar"<govind.bansal78@gov.in>, "RAJ KUMAR"<rkumar.edu@nic.in>, "RAKESH KUMAR" <rk.singh67@nic.in>, "PRIYADARSHIKA SRIVASTAVA"<priyadarshika.s@gov.in>, "Anjana Rajkumar"<director-cghs@cghs.nic.in>, "R.K. Singh"<rk.singh27@nic.in>, "Indranil Das"<indranil.das@gov.in>, "Dinesh Kumar" <dinesh.kumar14@nic.in>, "Nikhil Agarwal"<nikhilkr.agarwal@nic.in>, "Poonam Meena"<poonam.22@gov.in>, "Mrs Bharti Sahai"<bharti.sahai@nic.in>, "Noorin Bux Khan"<noorinbux@ord.gov.in>, "ghalmevc" <ghalme.vc@gov.in>, "naveenaggarwal"<naveen.aggarwal@ias.gov.in>, "Nidhi Kesarwani"<nidhikesarwani@nic.in>, "Bherav Dutt"<bherav.dutt@nic.in>, "Samsul Haque"<samsul.haque@nic.in>, "DR.PULKESH KUMAR" <dr.pulkesh@gov.in>, "Z. A. Khan"<us-doj@mha.gov.in>, "Manoj Kumar Sinha"<mk.sinha26@nic.in>, "Sarvajit Kumar"<kumar.sarvajit@nic.in>, "G A Raghuvanshi"<gopal.aaditya@nic.in>, "Sarita Nair"<sarita.nair@gov.in>, "Shri Raj Kumar Deputy Secretary"<raj.kumar28@nic.in>, "Rajesh Kumar verma"<rajeshkumar.verma@nic.in>, "KAMAL ARORA DS"<kamal.arora@nic.in>, "abhijit cgca"<abhijit.cgca@gov.in>, "KAUSTUBH GIRI"<dsnhmfin-mohfw@gov.in>, "NAVEEN AGGARWAL"<naveen.aggarwal@ias.nic.in>, "Aashima Bhatnagar" <aashima.bhatnagar@gov.in>, "Arvind Thakur"<arvind.thakur@nic.in>, "RAJENDRA PRASAD SATI DEPUTY SECRETARY"<rp.sati88@nic.in>
Cc: "PUNYA SALILA SRIVASTAVA"<secyhfw@nic.in>, "Madhukar Bhagat"<jsehealth-mohfw@gov.in>, "HarishKumarJain PPS"<harish.jain68@gov.in>, "REENA SHARMA"<reena.sharma80@gov.in>, "Pawan Kumar" <pawan.kumar13@nic.in>, "Avinash Yadav"<avinash.yadav73@gov.in>, "eHealth Section"<telmed-mohfw@gov.in>, "ehealthmohfw1"<ehealth.mohfw1@gmail.com>
Date: Fri, 08 Aug 2025 15:23:55 +0530
Subject: Cyber Security Advisory received From the National Critical Information Infrastructure Protection Centre (NCIIPC) reg.
========== Forwarded message ==========

Sir/Madam,

Kindly refer to the attached Cyber Security Advisory received from the National Critical Information Infrastructure Protection Centre (NCIIPC). This is for your information and necessary action, please.



Regards
eHealth Section
Ministry of Health & Family welfare
Room No.-213, D-wing, Nirman Bhawan
New Delhi-110011
Tel No.-23062263

2 attachments

Advisory No_ TA-MI-2025-08-07-001_ Malicious IOCs Targeting Critical Sectors [TLP_ AMBER].pdf
354K

Advisory No_ TA-PHI-2025-08-07-002_ Phishing Attack [TLP_ AMBER].pdf
298K

Fwd: Advisory No: TA-MI-2025-08-07-001: Malicious IOCs Targeting Critical Sectors [TLP: AMBER]

Madhukar Bhagat < jsehealth-mohfw@gov.in >

Thu, 07 Aug 2025 12:27:20 PM +0530

To "reenasharma80"<reena.sharma80@gov.in>

Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do he needful

o/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Thu, 07 Aug 2025 12:05:02 +0530
Subject: Advisory No: TA-MI-2025-08-07-001: Malicious IOCs Targeting Critical Sectors [TLP: AMBER]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-MI-2025-08-07-001

Cyber Security Advisory: Malicious IOCs Targeting Critical Sectors

This data is to be considered as TLP: AMBER

Based on analysis, please find below malicious IoCs targeting Critical Information Infrastructures (CII). Consider life span for malicious IP addresses at least 14 days.

**********IOC START**********

IPs:

159[.]223[.]35[.]231
49[.]15[.]230[.]14
188[.]166[.]197[.]157
8[.]218[.]33[.]227
118[.]194[.]228[.]15
8[.]219[.]194[.]246
188[.]166[.]199[.]119
8[.]222[.]158[.]127
8[.]222[.]223[.]100
198[.]98[.]57[.]26
8[.]219[.]174[.]2

103[.]100[.]223[.]183
8[.]222[.]236[.]85
152[.]58[.]186[.]109
8[.]219[.]176[.]208
106[.]219[.]88[.]16
46[.]148[.]26[.]94
8[.]222[.]129[.]108
8[.]219[.]221[.]108
8[.]219[.]176[.]71
182[.]40[.]118[.]5
8[.]219[.]6[.]240
8[.]222[.]167[.]136
8[.]219[.]6[.]61
104[.]239[.]177[.]48
8[.]213[.]199[.]168
111[.]67[.]203[.]251
8[.]222[.]163[.]222
8[.]219[.]157[.]184
8[.]219[.]182[.]182
8[.]219[.]143[.]16
8[.]219[.]207[.]144
8[.]219[.]180[.]252
8[.]222[.]187[.]219
8[.]222[.]184[.]84
8[.]219[.]90[.]95
152[.]58[.]187[.]203
8[.]219[.]133[.]204
47[.]236[.]226[.]89
47[.]237[.]11[.]22
118[.]182[.]79[.]13
152[.]59[.]147[.]166
8[.]222[.]252[.]209
8[.]213[.]207[.]174
8[.]209[.]197[.]243
8[.]222[.]132[.]133
8[.]219[.]9[.]3
8[.]216[.]86[.]134
204[.]76[.]203[.]193
8[.]219[.]72[.]29
36[.]133[.]15[.]139
8[.]219[.]151[.]215
8[.]213[.]40[.]177
8[.]222[.]249[.]19
8[.]219[.]217[.]42
77[.]239[.]217[.]216
8[.]133[.]255[.]12
8[.]219[.]6[.]49
8[.]219[.]249[.]135
8[.]219[.]146[.]174
45[.]135[.]194[.]11
8[.]219[.]212[.]37
8[.]222[.]137[.]9
47[.]79[.]21[.]25
8[.]222[.]233[.]13
8[.]219[.]8[.]115
178[.]72[.]81[.]86
8[.]222[.]193[.]52
47[.]237[.]173[.]37
8[.]219[.]230[.]6

47[.]93[.]212[.]99
8[.]209[.]211[.]125
8[.]219[.]103[.]48
8[.]222[.]218[.]12
8[.]219[.]168[.]13
211[.]101[.]235[.]68
27[.]43[.]204[.]70
8[.]222[.]215[.]216
8[.]219[.]244[.]167
45[.]125[.]66[.]95
38[.]59[.]219[.]27
107[.]189[.]31[.]150
159[.]89[.]211[.]52
122[.]97[.]209[.]209
59[.]91[.]174[.]229
112[.]94[.]99[.]39
154[.]90[.]63[.]89
27[.]43[.]205[.]204
181[.]177[.]141[.]165
36[.]255[.]7[.]25
27[.]47[.]3[.]218
221[.]13[.]232[.]95
154[.]12[.]224[.]130
202[.]168[.]85[.]66
120[.]85[.]143[.]27
36[.]255[.]5[.]189
120[.]85[.]92[.]26
103[.]42[.]243[.]181
38[.]211[.]193[.]130
120[.]85[.]112[.]227
103[.]42[.]243[.]197
172[.]20[.]30[.]114
139[.]59[.]223[.]9
59[.]88[.]157[.]153
103[.]152[.]159[.]123
114[.]66[.]56[.]37
43[.]249[.]192[.]179
217[.]156[.]122[.]189
36[.]255[.]5[.]95
223[.]149[.]1[.]80
120[.]85[.]114[.]213
36[.]41[.]154[.]118
192[.]183[.]232[.]142
110[.]171[.]195[.]49
59[.]126[.]193[.]88
45[.]153[.]34[.]206
157[.]230[.]193[.]102
89[.]190[.]84[.]147
141[.]98[.]10[.]150
92[.]241[.]100[.]218
125[.]228[.]34[.]185
77[.]243[.]118[.]197
223[.]171[.]75[.]106
117[.]121[.]234[.]122
46[.]64[.]6[.]123
101[.]178[.]217[.]24
125[.]228[.]251[.]128
46[.]200[.]52[.]200
78[.]186[.]71[.]142

61[.]0[.]41[.]133
184[.]163[.]26[.]176
123[.]193[.]229[.]217
180[.]176[.]248[.]63
39[.]108[.]62[.]29
111[.]173[.]105[.]184
51[.]210[.]9[.]101
124[.]218[.]87[.]180
47[.]197[.]17[.]145
143[.]208[.]124[.]111
185[.]17[.]20[.]48
61[.]61[.]186[.]149
84[.]46[.]245[.]2
211[.]23[.]129[.]69
59[.]120[.]251[.]51
220[.]133[.]203[.]190
122[.]117[.]69[.]95
59[.]124[.]156[.]78
118[.]248[.]226[.]131
58[.]35[.]15[.]87
98[.]19[.]89[.]43
103[.]158[.]171[.]55
180[.]159[.]40[.]90
88[.]162[.]67[.]91
114[.]35[.]63[.]99
122[.]116[.]160[.]140
114[.]33[.]242[.]234
79[.]11[.]187[.]8
45[.]153[.]34[.]225
49[.]213[.]163[.]69
62[.]213[.]164[.]145
116[.]241[.]112[.]124
80[.]232[.]247[.]146
81[.]88[.]213[.]187
106[.]1[.]81[.]42
110[.]171[.]195[.]96
79[.]34[.]255[.]41
27[.]193[.]153[.]227
85[.]130[.]182[.]17
183[.]230[.]190[.]11
190[.]80[.]88[.]225
76[.]170[.]132[.]63
223[.]171[.]39[.]117
94[.]243[.]9[.]176
74[.]140[.]111[.]157
203[.]172[.]208[.]236
184[.]22[.]101[.]9
66[.]146[.]109[.]88
185[.]143[.]205[.]224
24[.]61[.]198[.]121
223[.]171[.]75[.]171
223[.]171[.]54[.]197
168[.]220[.]165[.]153
24[.]91[.]100[.]164
61[.]216[.]112[.]71
185[.]17[.]133[.]45
59[.]126[.]184[.]163
223[.]171[.]65[.]191
173[.]217[.]170[.]41

78[.]187[.]50[.]160
139[.]5[.]1[.]68
114[.]35[.]57[.]126
95[.]9[.]44[.]188
46[.]254[.]166[.]76
59[.]127[.]187[.]82
176[.]58[.]69[.]88
125[.]229[.]204[.]96
157[.]15[.]66[.]141
67[.]186[.]225[.]89
185[.]43[.]16[.]171
218[.]161[.]49[.]136
95[.]104[.]22[.]209
203[.]106[.]109[.]145
188[.]72[.]6[.]126
120[.]86[.]238[.]230
220[.]134[.]137[.]233
109[.]115[.]114[.]166
125[.]229[.]182[.]249
71[.]65[.]214[.]218
70[.]80[.]175[.]4
120[.]86[.]252[.]35
85[.]99[.]113[.]207
223[.]171[.]42[.]251
76[.]129[.]94[.]167
122[.]117[.]250[.]106
114[.]32[.]217[.]180
115[.]134[.]129[.]81
171[.]99[.]190[.]87
175[.]17[.]14[.]30
50[.]122[.]118[.]166
49[.]158[.]240[.]17
173[.]242[.]142[.]141
94[.]69[.]234[.]122
45[.]135[.]197[.]213
49[.]213[.]239[.]228
36[.]255[.]7[.]67
85[.]105[.]177[.]136
123[.]241[.]76[.]55
61[.]57[.]69[.]111
2[.]81[.]15[.]188
218[.]35[.]166[.]63
171[.]103[.]78[.]130
96[.]56[.]41[.]131
80[.]119[.]24[.]90
171[.]37[.]48[.]238
95[.]9[.]141[.]201
223[.]149[.]162[.]115
114[.]35[.]242[.]196
85[.]221[.]255[.]216
103[.]99[.]196[.]16
211[.]22[.]140[.]17
210[.]187[.]178[.]141
120[.]85[.]92[.]219
61[.]65[.]124[.]67
1[.]81[.]198[.]28
220[.]133[.]222[.]252
178[.]176[.]48[.]232
58[.]37[.]225[.]174

103[.]199[.]205[.]90
79[.]2[.]83[.]111
124[.]120[.]8[.]159
123[.]194[.]54[.]147
203[.]204[.]242[.]145
114[.]35[.]102[.]249
101[.]128[.]75[.]52
125[.]229[.]221[.]223
70[.]53[.]247[.]83
93[.]170[.]112[.]216
114[.]35[.]230[.]84
125[.]229[.]191[.]84
144[.]172[.]110[.]50
69[.]143[.]111[.]251
199[.]188[.]125[.]166
175[.]20[.]41[.]33
59[.]125[.]251[.]160
120[.]85[.]185[.]236
178[.]131[.]93[.]188
88[.]249[.]41[.]206
103[.]168[.]2[.]105
175[.]139[.]33[.]169
90[.]146[.]186[.]137
213[.]78[.]110[.]78
58[.]35[.]209[.]210
75[.]97[.]133[.]250
117[.]235[.]42[.]42
114[.]35[.]126[.]195
68[.]196[.]145[.]221
185[.]213[.]240[.]143
78[.]80[.]32[.]202
77[.]239[.]216[.]31
103[.]173[.]211[.]76
128[.]116[.]206[.]185
125[.]229[.]143[.]219
87[.]121[.]84[.]132
110[.]171[.]184[.]92
185[.]130[.]24[.]164
91[.]175[.]68[.]205
139[.]5[.]10[.]201
120[.]85[.]119[.]149
117[.]205[.]164[.]112
184[.]22[.]89[.]220
103[.]238[.]200[.]34
173[.]90[.]117[.]154
27[.]43[.]205[.]121
218[.]161[.]92[.]94
38[.]43[.]198[.]157
220[.]133[.]161[.]244
102[.]212[.]40[.]118
175[.]107[.]0[.]77
116[.]58[.]181[.]209
120[.]85[.]182[.]63
223[.]171[.]65[.]136
123[.]113[.]152[.]239
220[.]132[.]196[.]159
110[.]171[.]195[.]211
59[.]127[.]112[.]199
223[.]171[.]51[.]205

58[.]37[.]129[.]214
32[.]220[.]1[.]61
106[.]1[.]20[.]89
78[.]134[.]60[.]205
223[.]171[.]54[.]239
87[.]15[.]114[.]112
89[.]221[.]203[.]116
172[.]94[.]96[.]217
107[.]189[.]27[.]205
83[.]252[.]42[.]112
103[.]160[.]197[.]42
27[.]194[.]149[.]124
156[.]244[.]19[.]33
59[.]97[.]252[.]55
27[.]43[.]204[.]110
36[.]255[.]5[.]97
59[.]97[.]250[.]153
45[.]125[.]15[.]101
103[.]160[.]197[.]74
114[.]246[.]35[.]22
120[.]86[.]238[.]242
146[.]190[.]6[.]108
157[.]230[.]43[.]138
198[.]38[.]88[.]21
207[.]167[.]64[.]12
209[.]141[.]55[.]55

URLs:
hxxp://117[.]200[.]127[.]129:53527/
hxxp://117[.]254[.]97[.]154:43565/
hxxp://117[.]198[.]13[.]34:58921/
hxxp://117[.]204[.]167[.]67:43042/
hxxp://117[.]200[.]81[.]222:39133/
hxxp://117[.]205[.]81[.]235:58803/
hxxp://103[.]42[.]157[.]141:37520/
hxxp://117[.]217[.]40[.]52:42736/
hxxp://175[.]107[.]1[.]250:60056/
hxxp://102[.]33[.]43[.]146:43977/
hxxp://218[.]62[.]247[.]171:33178/
hxxp://103[.]93[.]93[.]181:59678/
hxxp://45[.]230[.]66[.]114:10110/
hxxp://39[.]89[.]9[.]191:50751/
hxxp://103[.]93[.]93[.]181:59270/
hxxp://180[.]190[.]188[.]205:52911/
hxxp://45[.]230[.]66[.]98:11695/
hxxp://45[.]230[.]66[.]115:11048/
hxxp://219[.]157[.]50[.]25:34471/
hxxp://42[.]178[.]181[.]199:47738/
hxxp://59[.]88[.]153[.]215:58965/
hxxp://139[.]5[.]10[.]14:52239/
hxxp://103[.]160[.]197[.]97:43237/
hxxp://60[.]22[.]100[.]77:38563/
hxxp://139[.]5[.]0[.]54:47107/
hxxp://103[.]207[.]224[.]212:34883/
hxxp://59[.]88[.]137[.]153:60639/
hxxp://42[.]225[.]207[.]38:40794/
hxxp://117[.]205[.]84[.]216:34767/
hxxp://119[.]123[.]46[.]109:39034/
hxxp://61[.]70[.]84[.]40:55300/

hxxp://103[.]199[.]180[.]68:47788/
hxxp://103[.]199[.]200[.]188:32831/
hxxp://45[.]230[.]66[.]96:10301/
hxxp://152[.]252[.]65[.]74:49583/
hxxp://117[.]198[.]14[.]202:52174/
hxxp://45[.]230[.]66[.]110:10454/
hxxp://103[.]160[.]197[.]221:45971/
hxxp://103[.]158[.]171[.]53:34405/
hxxp://117[.]219[.]147[.]123:40109/
hxxp://27[.]157[.]144[.]228:41048/
hxxp://42[.]5[.]249[.]7:46678/
hxxp://183[.]108[.]45[.]84:46803/
hxxp://103[.]199[.]200[.]253:49815/
hxxp://60[.]23[.]77[.]112:60687/
hxxp://117[.]211[.]34[.]14:37939/
hxxp://45[.]230[.]66[.]110:11110/
hxxp://103[.]152[.]159[.]68:52210/
hxxp://114[.]66[.]56[.]37:19490/
hxxp://unjiproxy[.]p-e[.]kr:6969/selftbk[.]sh
hxxp://192[.]183[.]232[.]142/rondo[.]zqq[.]sh
hxxp://103[.]98[.]38[.]82:35262/
hxxp://103[.]152[.]159[.]235:60732/
hxxp://113[.]205[.]248[.]18:41755/
hxxp://59[.]96[.]137[.]225:52432/
hxxp://45[.]230[.]66[.]113:11076/
hxxp://45[.]230[.]66[.]122:10804/
hxxp://117[.]235[.]60[.]53:56923/
hxxp://61[.]3[.]135[.]10:33776/
hxxp://45[.]230[.]66[.]99:10667/
hxxp://103[.]168[.]2[.]253:58302/
hxxp://42[.]235[.]67[.]49:52060/
hxxp://182[.]127[.]53[.]56:48890/
hxxp://112[.]248[.]187[.]86:57659/
hxxp://42[.]234[.]203[.]101:49073/
hxxp://59[.]88[.]38[.]96:44469/
hxxp://103[.]199[.]200[.]214:48496/
hxxp://89[.]67[.]208[.]28:36661/
hxxp://162[.]250[.]16[.]20:43993/
hxxp://117[.]206[.]16[.]146:38840/
hxxp://115[.]50[.]80[.]246:60849/
hxxp://112[.]232[.]169[.]254:57012/
hxxp://45[.]230[.]66[.]106:11142/
hxxp://103[.]110[.]16[.]168:51212/
hxxp://103[.]197[.]113[.]120:51317/
hxxp://157[.]15[.]66[.]140:48114/
hxxp://103[.]93[.]93[.]178:52743/
hxxp://117[.]209[.]86[.]31:39679/
hxxp://139[.]5[.]11[.]207:53273/
hxxp://117[.]209[.]95[.]169:36378/
hxxp://45[.]230[.]66[.]98:11855/
hxxp://103[.]207[.]224[.]133:51821/
hxxp://182[.]235[.]148[.]10:53760/
hxxp://45[.]230[.]66[.]116:10735/
hxxp://182[.]124[.]11[.]164:56085/
hxxp://45[.]230[.]66[.]117:10176/
hxxp://90[.]150[.]75[.]234:46932/
hxxp://103[.]99[.]196[.]165:46610/
hxxp://139[.]5[.]10[.]209:51744/
hxxp://115[.]49[.]203[.]237:51784/

hxxp://177[.]92[.]240[.]168:53408/
hxxp://59[.]97[.]253[.]114:33267/
hxxp://182[.]119[.]60[.]212:59407/
hxxp://103[.]208[.]105[.]170:55717/
hxxp://45[.]230[.]66[.]101:11333/
hxxp://42[.]58[.]169[.]180:52223/
hxxp://117[.]235[.]52[.]181:33875/
hxxp://45[.]230[.]66[.]118:11403/
hxxp://163[.]123[.]19[.]88:50813/
hxxp://59[.]174[.]119[.]6:40205/
hxxp://103[.]93[.]93[.]182:54895/
hxxp://125[.]72[.]194[.]174:43742/
hxxp://59[.]97[.]251[.]158:43291/
hxxp://61[.]1[.]232[.]114:57818/
hxxp://117[.]213[.]240[.]155:35990/
hxxp://222[.]140[.]78[.]126:60900/
hxxp://112[.]198[.]129[.]201:52310/
hxxp://103[.]48[.]66[.]170:55071/
hxxp://61[.]1[.]236[.]61:35954/
hxxp://103[.]207[.]224[.]209:46939/
hxxp://93[.]119[.]134[.]224:55453/
hxxp://45[.]230[.]66[.]104:11433/
hxxp://31[.]162[.]19[.]189:58570/
hxxp://89[.]221[.]203[.]116:6969/
hxxp://59[.]88[.]232[.]58:51068/
hxxp://103[.]93[.]93[.]178:36331/
hxxp://192[.]21[.]160[.]101:40099/
hxxp://89[.]67[.]72[.]201:56101/
hxxp://117[.]247[.]145[.]222:42021/
hxxp://115[.]183[.]49[.]93:41554/
hxxp://183[.]135[.]201[.]177:49822/
hxxp://59[.]97[.]250[.]153:46861/
hxxp://221[.]200[.]218[.]88:49549/
hxxp://117[.]216[.]60[.]224:56097/
hxxp://117[.]205[.]83[.]40:57858/
hxxp://59[.]98[.]119[.]67:51262/
hxxp://45[.]230[.]66[.]96:11787/
hxxp://123[.]190[.]191[.]183:53785/
hxxp://103[.]98[.]38[.]235:47440/
hxxp://172[.]59[.]82[.]220:33904/
hxxp://103[.]93[.]93[.]182:39678/
hxxp://117[.]216[.]183[.]9:36955/

**********IOC END**********

Recommendation:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.

Note: TA-MI: Threat Alert Malicious IOCs

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: AMBER. Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

---

advisory@nciipc.gov.in mailing list

Fwd: Advisory No: TA-PHI-2025-08-07-002: Phishing Attack [TLP: AMBER]

Madhukar Bhagat < jsehealth-mohfw@gov.in >
Thu, 07 Aug 2025 3:23:02 PM +0530

To "reenasharma80"<reena.sharma80@gov.in>
Cc "Pawan Kumar"<pawan.kumar13@nic.in>,"eHealth Section"<telmed-mohfw@gov.in>

Mam/Sir

Pl do he needful

o/oJS(MKB)
23061066

========== Forwarded message ==========
From: Advisory NCIIPC <advisory@nciipc.gov.in>
Date: Thu, 07 Aug 2025 15:09:12 +0530
Subject: Advisory No: TA-PHI-2025-08-07-002: Phishing Attack [TLP: AMBER]
========== Forwarded message ==========

Government of India

National Critical Information Infrastructure Protection Centre

(A Unit of NTRO)

Advisory No: TA-PHI-2025-08-07-002

Cyber Security Advisory: Phishing Attack

This data is to be considered as TLP: AMBER

It has been observed that government personnel have received phishing emails from spoofed / compromised email IDs and malicious domains. The email contains an archive file named " Meeting_Ltr_ID1543ops.pdf.zip". Upon clicking the archive file, "Meeting_Ltr_ID1543ops.pdf.desktop" is extracted which is malicious file and on clicking, " Meeting_Ltr_ID1543ops.pdf.desktop" file, a PDF file named " Nomination.pdf" is downloaded from the link ' hxxps://drive.google[.]com/file/d/1cAEBP1C4ujKbzF4Ji_yknFbP1GR9oXi/view?usp=sharing' and opened which is not malicious but decoy used to convince the victim of the legitimacy of the mail. Simultaneously multiple commands get executed in the background. These commands download "Mt_dated_29.txt" from link "hxxps://securestore[.]cv/ghg/Mt_dated_29.txt" . The "Mt_dated_29.txt" contains binary code of ELF file and in the background it download and execute ELF(Executable linkable File) file "Meeting_Ltr_ID1543ops.pdf". The ELF file named "Meeting_Ltr_ID1543ops.pdf", is an executable as Password Stealer malware. Its primary function is to target and extract stored browser data, including saved credentials, and transmit the stolen information to the domain "hxxp://modgovindia[.]space/"

Mitre ATT&CK Tactics and Techniques:

- TA0002: Execution
  - T1059: Scheduled Task/Job
  - T1064: Scripting
- TA0003: Persistence
  - T1059: Scheduled Task/Job
  - T1059: Create or Modify System Process
  - T1546: Event Triggered Execution
  - T1546.004: Unix Shell Configuration Modification
- TA0007: Discovery
  - T1518.001: Security software Discovery.
  - T1518: Software Discovery
  - T1222: File and Discovery
- TA0004: Privilege Escalation
  - T1059: Scheduled Task/Job
  - T1059: Create or Modify System Process
  - T1546: Event Triggered Execution
  - T1546.004: Unix Shell Configuration Modification
- TA0005: Defense Evasion
  - T1064: Scripting
  - T1222: File and Directory Permissions Modification
  - T1064: Hide Artifacts
  - T1564.001: Hidden Files and Directories
- TA0007: Discovery
  - T1064: Scripting
  - T1222: File and Directory Permissions Modification
  - T1547.001: Plist Modifaction.
  - T1574.002: DLL side Loading
- TA0010: Exfiltration
  - T1048: Exfiltration Over Alternative Protocol
- TA0011 : Command and Control
  - T1071: Application Layer Protocol.
  - T1095 : Non-Application Layer Protocol.
  - T1571: Non-Standard Port

**********IOC START**********

Filename:
Meeting_Ltr_ID1543ops.pdf.zip
Hashes:
32b56830974b96a3379866d12410fa96
4c2f6c87a301a06f7cb5b41ebd2454ac86589596
508a2bcaa4c511f7db2d4491bb76effaa7231d66110c28632b95c77be40ea6b1

Filename:
Meeting_Ltr_ID1543ops.pdf.desktop
Hashes:
10b7139952e3daae8f9d7ee407696ccf
f2ada639ba011727b5036c804e30ca37cb61d432
8f8da8861c368e74b9b5c1c59e64ef00690c5eff4a95e1b4fcf386973895bef1

Filename:
Meeting_Ltr_ID1543ops.pdf-
Hashes:
5bfeeae3cc9386513dc7c301c61e67a7
bcef7d3ca12afa877467efc078d9c80c0ea5d242

e689afee5f7bdbd1613bd9a3915ef2a185a05c72aaae4df3dee988fa7109cb0b

Domains:
securestore[.]cv
modgovindia[.]space

IPs:
184.94.213[.]23
45.141.58[.]199

**********IOC END**********

Recommendations:

- It is recommended that organisations should apply the given IoCs on their security systems to identify attacks. Occurrence of any communication traces pertaining to these IoCs may be reported to NCIIPC.
- Install and regularly update antivirus software.
- Install Updates and Patches regularly.
- Conduct regular backup practices and keep those backups offline or on a separate network.
- Implement Multi-Factor Authentication (MFA).
- Never click and execute email attachments from unknown sources.
- Never open links shared on social media from unknown sources.
- Never run unknown files with exaggerated titles.
- Users of nic.in and gov.in domains be sensitised about the threat vector.

Note: *TA-PHI: Threat Alert Phishing Advisory*

With Best Regards,
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430

This document is distributed as TLP: AMBER. Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

advisory@nciipc.gov.in mailing list

MOST IMMEDIATE

No. Z-28016/77/2025-PMSSY-I (EO 8348485)
Government of India
Ministry of Health and Family Welfare
Department of Health & Family Welfare
PMSSY Division

Nirman Bhawan, New Delhi
Dated: 16th July, 2025.

To

The Executive Director,
All India Institute of Medical Sciences (AIIMS)
(All AIIMS under PMSSY)

Subject: Implementation of SAKSHAM – Learning Management Information System (LMIS) developed by NIHFW – reg.

Sir/Madam,

I am directed to refer to the launch of SAKSHAM (Stimulating Advanced Knowledge for Sustainable Health Management), a Learning Management Information System (LMIS) developed by the National Institute of Health and Family Welfare (NIHFW), New Delhi and formally launched by the Union Health Secretary on 10th May 2023.

2. SAKSHAM-LMIS is a national-level digital platform aimed at capacity building of healthcare professionals across all levels—from rural Primary Health Centres to tertiary care hospitals. It provides access to a wide range of online training and certification courses, currently hosting over 200 public health and 100 clinical modules. Health professionals can register and participate via the portal at https://lmis.nihfw.ac.in. or https://nihfw-dev.inroad.in/. For any specific query, Institutes are requested to contact NIHFW at their mail ID lmis.nihfw@gmail.com.

3. It has been observed that some AIIMS set up under PMSSY are using SAKSHAM-LMIS however in some others like AIIMS Gorakhpur, Guwahati, Rajkot and Mangalagiri either the process of on-boarding has not started or is under process. It is also not clear whether the full potential of this platform has been optimised by the Institutes using SAKSHAM . In order to ensure effective implementation of this platform across all AIIMS, the following action points are advised:

i. Each AIIMS to nominate a Nodal Officer to coordinate SAKSHAM implementation and interface with NIHFW and the Ministry.
ii. Conduct internal sensitization programs/webinars for students, medical faculty, residents, and paramedical staff to promote enrollment.
iii. Institutes may explore incorporating relevant SAKSHAM modules into internal training programs or CME initiatives.
iv. Participants may be encouraged to submit feedback on course quality and utility to NIHFW for continuous platform improvement.

4. In view of above, it is requested to kindly initiate necessary action in this regard under intimation to the Ministry .

Yours faithfully,

(Raj Kumar)
Dy. Secretary, PMSSY-I
Ministry of Health and Family Welfare
[011-23063178]
✉ Email: [raj.kumar23@nic.in]

Digitally signed by Raj Kumar
Date: 16.07.2025 16:39:13

Copy to:

1. PPS to Secretary (HFW) – for kind information.
2. JS (PMSSY), MoHFW – for kind information.

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Seeking clarification regarding applicability of Reservation Roster for filling up of some posts by promotion at AIIMS, Patna - reg

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Wed, Dec 17, 2025 at 3:23 PM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **DDA AIIMS PATNA** <dda@aiimspatna.org>
Date: Fri, Jul 25, 2025 at 11:09 AM
Subject: Fwd: Seeking clarification regarding applicability of Reservation Roster for filling up of some posts by promotion at AIIMS, Patna - reg
To: Amit Kumar Sinha <amit.sinha@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **Director .** <director@aiimspatna.org>
Date: Wed, 23 Jul 2025, 17:44
Subject: Fwd: Seeking clarification regarding applicability of Reservation Roster for filling up of some posts by promotion at AIIMS, Patna - reg
To: DDA AIIMS PATNA <dda@aiimspatna.org>

Sd/-
Prof. (Dr.) Saurabh Varshney
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109

---------- Forwarded message ---------
From: **pmssysection iv** <pmssysectioniv@gmail.com>

Date: Wed, Jul 23, 2025 at 4:32 PM
Subject: Seeking clarification regarding applicability of Reservation Roster for filling up of some posts by promotion at AIIMS, Patna - reg
To: Director Patna <director@aiimspatna.org>
Cc: DDA AIIMS PATNA <dda@aiimspatna.org>, : <Ak.biswas57@nic.in>, Devender DKumarGothal <dev.gothal@gov.in>, <a.adil60@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officers of PMSSY-IV Section at - ;ak.biswas57@nic.in; dev.gothal@gov.in; a.adil60@gov.in;

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

Letter (80).pdf
96K

No. Z-28016/59/2025-PMSSY-V
Government of India
Ministry of Health & Family Welfare
(PMSSY-IV Section)
*****

745-A, 7th Floor, Nirman Bhawan, New Delhi
Dated 23-07-2025

To,

The Executive Director,
AIIMS Patna

Subject: Seeking clarification regarding applicability of Reservation Roster for filling up of some posts by promotion at AIIMS, Patna - reg.

Sir,

I am directed to refer to AIIMS Patna's letter No. F-201023/AIIMS/Pat/Admin./2005 dated 17.02.2025 on the above mentioned subject and advise to take action in the matter as per the instructions/guidelines issued by DOPT time to time and with the approval of GB/IB.

Yours faithfully,
Digitally signed by
ARUN KUMAR BISWAS
Date: 23-07-2025
09:38:11

(Arun Kumar Biswas)
Under Secretary to the Govt. of India
Tel.011-23061343

Copy to: DD (A), AIIMS, Patna

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Cyber Security Guidelines for new AIIMS/INIs-reg.

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Wed, Dec 17, 2025 at 3:20 PM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **Director .** <director@aiimspatna.org>
Date: Tue, Jul 29, 2025 at 5:05 PM
Subject: Fwd: Cyber Security Guidelines for new AIIMS/INIs-reg.
To: DDA AIIMS PATNA <dda@aiimspatna.org>

Sd/-
Prof. (Dr.) Saurabh Varshney
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109

---------- Forwarded message ---------
From: **SUBHANSHU KUMAR** <subhanshu.kumar@gov.in>
Date: Tue, Jul 29, 2025 at 3:38 PM
Subject: Cyber Security Guidelines for new AIIMS/INIs-reg.
To: director <director@aiimsbhopal.edu.in>, director <director@aiimsbhubaneswar.edu.in>, director <director@aiimsjodhpur.edu.in>, director <director@aiimspatna.org>, director <director@aiimsraipur.edu.in>, director <director@aiimsrishikesh.edu.in>, director <director@aiimsmangalagiri.edu.in>, directoraiimsnagpur <directoraiimsnagpur@gmail.com>, drppjoshi <drppjoshi@aiimsnagpur.edu.in>, edaiimsrbl <edaiimsrbl@gmail.com>, executivedirector <executivedirector@aiimsgorakhpur.edu.in>, ed <ed@aiimskalyani.edu.in>, director <director@aiimsdeoghar.edu.in>, director <director@aiimsbibinagar.edu.in>, director <director@aiimsbilaspur.edu.in>, sharmadn <sharmadn@aiims.edu>, shakti810505 <shakti810505@gmail.com>, director <director@aiimsjammu.edu.in>, drmhraosvims1957 <drmhraosvims1957@gmail.com>, director <director@aiimsguwahati.ac.in>, madhabananda <madhabananda@gmail.com>, sachimohanty <sachimohanty@rediffmail.in>, dpgi <dpgi@pgimer.edu.in>, director <director@jipmer.ac.in>, director <director@aiims.gov.in>, dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsraipur.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, dda <dda@aiimsjodhpur.edu.in>, dda <dda@aiimspatna.org>, dda <dda@aiimsrishikesh.edu.in>, rajeevsenroy30 <rajeevsenroy30@gmail.com>, dda <dda@aiimsbathinda.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, ddaaiimsrbl <ddaaiimsrbl@gmail.com>, kpradip10 <kpradip10@gmail.com>, dda <dda@aiimskalyani.edu.in>, dda <dda@aiimsgorakhpur.edu.in>, dda <dda@aiimsdeoghar.edu.in>, officeaiimsdeoghar <office.aiimsdeoghar@gmail.com>, ddaaiimsbibinagar <dda.aiimsbibinagar@gmail.com>, dda <dda@aiimsbibinagar.edu.in>, dda <dda@aiimsbilaspur.edu.in>, macprasad <mac.prasad@gmail.com>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, aps101982 <aps101982@rediffmail.com>, ddaaiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, aoaiimsmadurai <ao.aiimsmadurai@gmail.com>, dda <dda@aiimsguwahati.ac.in>, ddaaiimsawantipora1 <ddaaiimsawantipora1@gmail.com>, ddapgi <ddapgi@gmail.com>, krishanagoyal <krishana.goyal@jipmer.edu.in>

DDA <DDA@aiims.edu>
Cc: Shri Raj Kumar Deputy Secretary <raj.kumar28@nic.in>, dharmenderkumar14 <dharmender.kumar14@gov.in>, Ravi Kumar <ravi.kumar89@gov.in>

Respected Sir/Madam,

Please find the attachment on the subject cited above for necessary action.

With Regards,
Subhanshu Kumar
ASO (PMSSY-I)
MoHFW

---

6 attachments

letter to AIIMSINIs regarding cyber security guidelinesdated 28.07.2025.pdf
141K

MoHFWs letter to AIIMS dated 28.05.2025.pdf
79K

Model Cyber Security Plan for AIIMSINIs (shared by CIRA).pdf
4377K

National Cyber Security Policy- 2013 (issued by Meity).pdf
301K

Defence in Depth Strategy.pdf
1952K

Standard Operating Procedure Critical Sector Entities received from cyber wing of NSCS.pdf
1017K

CONFIDENTIAL

No. V-16020/67/2025-INI-I (E.O. No. 8334193)
Government of India
Ministry of Health and Family Welfare
Department of Health and Family Welfare
(PMSSY-I Section)

Nirman Bhawan, New Delhi
Dated: 28-07-2025

To,

The Director/Executive Director,
AIIMS New Delhi/INIs/ All New AIIMS under PMSSY.

Subject: Cyber security guidelines for new AIIMS/ INIs-reg.

Sir/ Madam,

I am directed to refer to this Ministry's letter of even number dated 28.05.2025, vide which the Model Cyber Security Plan for AIIMS/INIs (shared by CIRA) and National Cyber Security Policy-2013 (issued by MeitY) was circulated.

2. Further, I am directed to forward a copy of"Defence in Depth" Strategy which was discussed during Good Practices Conclave at AIIMS Nagpur on 13-14 June, 2025 and a copy of the Standard Operating Procedure Critical Sector Entities received from Cyber Wing of National Security Council Secretariat (NSCS).

3. The Office of Advisor (Cyber) has shared a"Defence in Depth Strategy" for securing healthcare systems, addressing protection of Protected Health Information (PHI), patient safety, and continuity of services. The key recommendations are:

(a) Implementation of layered security controls across distinct security domains.

(b) Establishment of specialized healthcare cybersecurity governance aligned with regulatory requirements.

(c) Deployment of medical device-specific security measures.

(d) Creation of 24x7 healthcare-focused Security Operations Centres (SOCs).

(e) Development of incident response capabilities prioritizing patient safety.

(f) Formulation of National Standards and following of prevalent international standards until national standards are formed

3. Additionally, the Cyber Wing of NSCS has issued a SOP for Critical Sector Entities in light of increasing threats to national digital infrastructure following the Pahalgam incident and Operation Sindoor. The SoP identifies 23 action points to be implemented by critical sectors to safeguard Indian cyberspace like action on

alerts & advisories, backup critical data, reporting of incidents, access controls,employee sensitization and monitoring, cyber drills, etc.

4. It is, therefore, requested to implement the guidelines and share compliance status with PMSSY Division within 30 days.

(Encl: As above)

Yours faithfully,

Digitally signed by RAJ KUMAR
Date: 28-07-2025 11:52:25

(Raj Kumar)
Deputy Secretary to the Govt. of India
Tel: 011-23063178
E-mail: raj.kumar28@nic.in

Copy to:-

1. Dy. Director (Admn.) of all concerned AIIMS/INIs
2. e-Health Section, MoH&FW
3. Director (INI)
4. US (INI-1/INI-2)

Copy for information to:-

PSO to JS(PMSSY)

V-16020/67/2025-INI-I
Government of India
Ministry of Health and Family Welfare
PMSSY-I

Nirman Bhawan, New Delhi
Dated: 28-05-2025

To

Directors/Executive Directors
All new AIIMS

Subject: Model IT Infra plan for new AIIMS/ INIs-reg.

Sir/Ma'am

I am directed to refer to subject cited above and forward herewithModel Cyber Security Plan for AIIMS/INIs shared by CIRA (Copy enclosed) along with National Cyber Security Policy-2013 issued by MeitY (copy enclosed) for information and taking further necessary action.

2. This issues with the approval of the competent authority.

Encl: As above.

Yours faithfully

Digitally signed by Raj Kumar
Date: 28-05-2025 09:39:10

(Raj Kumar)
Deputy Secretary to GoI
Tele: 011-23063178

Copy to:
1. DDA, All new AIIMS
2.All Division Heads of PMSSY Division

File No. V-16020/67/2025-INI-I (Computer No. 8334193)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 29/07/2025 02:46 pm

Advisor (Cyber)/S(01)/2024/568 dt. 09/09/2024

Annexure D

Model Cyber Security Plan for MoHFW Constituents

1. Introduction:

All Hospitals/Medical Institutes deal with a lot of digitization owing to online booking, consultations and medical services & hence it is important to enhance the infrastructure's *Network Capacity and cyber security capabilities* , thus improving the *Security Posture* in the most effective and non-disruptive way possible.

Some of the guiding principles that these institutes need to align with in order to realize the aforementioned objective are:

- Best possible healthcare to patients visiting Hospital.
- Data safety of Personally Identifiable Information (PII) and Protected Health Information (PHI) of all patients visiting Hospital.
- Availability of online services such as Online Registration System (ORS), academic resources etc., as well as off-campus access to healthcare data.
- Efficient IT operations and security management.
- Enhanced network performance and scalability.

2. Best Practices:

Keeping up with cyber security threats has always been a challenge, but today the speed at which new threats are introduced is astounding. The sophistication of attacks and the use of advanced tools like artificial intelligence, machine learning, and other technologies are making ransomware, phishing, and other known forms of attacks more prevalent.

When it comes to security in healthcare, it's clear that uncertainty has become the new normal. Many organizations are not sure how to identify and manage digital risks in the ever-changing threat landscape, and their current risk management strategies just can't keep up. Cyber security breaches for healthcare organizations don't just have a negative impact on the financial and reputational standings of a healthcare organization. Breaches can involve the theft of protected health information (PHI) and personal identifiable information (PII), and can also result in longer patient stays, delays in procedures, and diversions to other facilities.

Medical device security is also a concern for healthcare providers, as bad actors take aim at vulnerable unpatched systems and improperly configured devices. We know that connected medical devices can represent a large percentage of the devices on a Healthcare Delivery Organization's (HDO) network. The proliferation of smart and connected medical devices will only continue as we see shifts in sites of care (from acute and post-acute sites to non-acute sites and home-based services).

1.4.1 Main Network

Main network should implement the 3-tier hierarchical wired and wireless LAN as per industry best practices to ensure resilient LAN infrastructure of Hospital.

File No. V-16020/82/2024-INH (Computer No. 8[illegible])
Generated from eOffice by [illegible] on 29/07/2025 02:48 pm

1.4.2 Guest WLAN

A physically separate Guest WLAN network should be established to provide internet access to guest users. The guests (Patients/Attendants) shall be provided access to internet through the captive portal. The captive portal shall provide temporary network access to guest users while maintaining security. This approach is particularly useful in organizations with a high volume of visitors. Guest WLAN components shall include (but not limited to):

1. Next generation Firewall
2. DNS, DHCP and IP address management services.
3. SMS based authentication
4. Captive portal based Wi-Fi internet access
5. Log server for keeping access logs

3. Architecture:

The design has two physically separate networks. First is Main network and second is Guest WLAN network.

1.5.1 Main Network

The main network provides connectivity to access CII and Non CII applications hosted in data centre, cloud hosted applications, limited & controlled Internet access, Wi-Fi Network access and other office functions for Hospital users.

The below Figure shows the Main Network Logical Topology.

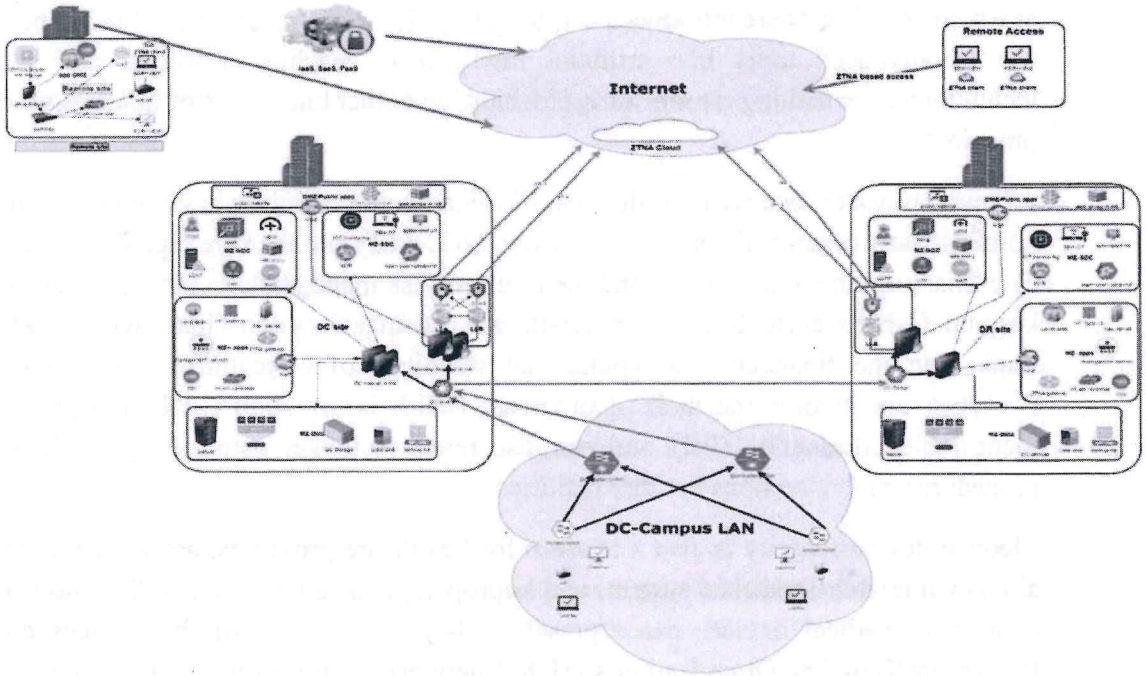


Figure 1: Main network logical Topology

* The main network Wi-Fi and guest WLAN Wi-Fi should be physically separate and non over lapping. Also, air-gap should be maintained between Operational network and Internet network.

File No. V-16020/82/2025/INI-I (Computer No. [illegible])
Generated from eOffice by [illegible] on 29/07/2025 02:48 pm
524

1.5.2 Guest WLAN

The Guest WLAN caters to needs of Hospital Guest users i.e., Patients and attendants for internet services. Below Figure shows the Guest WLAN logical topology.

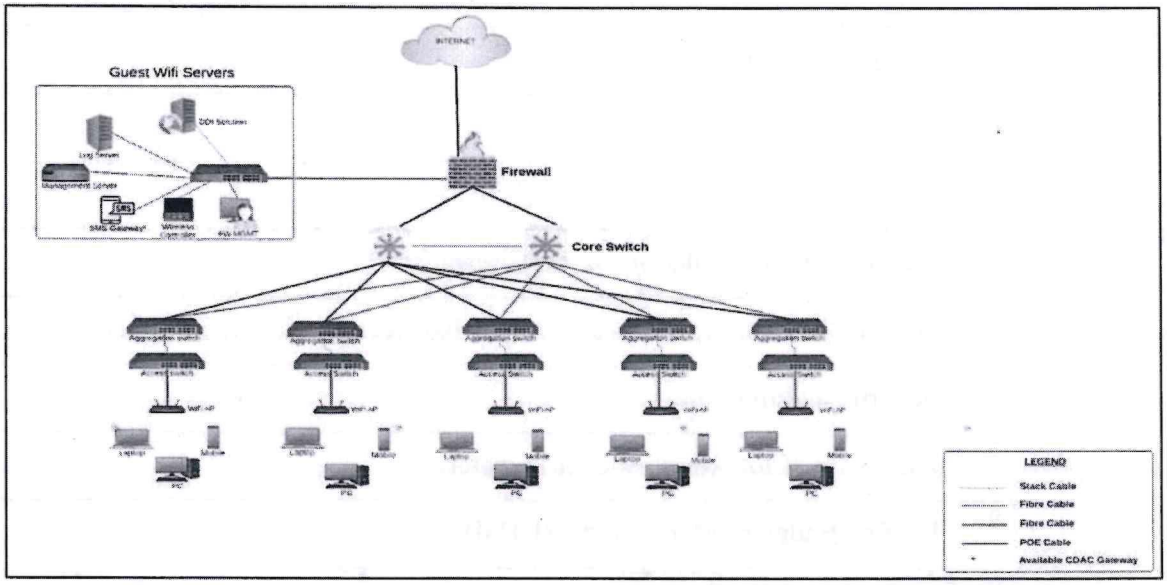


Figure 2: Guest WLAN Logical Topology

Necessary security measures have been proposed to ensure data security, redundancy, availability and backup. However as best practise it is recommended to review Hospital IT and Cyber security infrastructure periodically and update it as per latest security recommendations.

4. Cyber Security operations centre (SOC)

A security operations centre, or SOC, is a team of expert individuals and the facility in which they dedicate themselves entirely to high-quality IT security operations. A SOC seeks to prevent cyber security threats and detects and responds to any incident on the computers, servers and networks it oversees. What makes a SOC unique is the ability to monitor all systems on an on-going basis, as employees work in shifts, rotating and logging activity around the clock.

The SOC team stays ahead of potential threats by analysing active feeds, establishing rules, identifying exceptions, enhancing responses and keeping a close eye on possible vulnerabilities in the defences they have already set up. Ensuring these programs comply with company, industry and government regulations is also a significant part of a SOC's job.

Through their active surveillance and analysis, SOCs use strategic methodologies and processes to build and maintain the organization's cyber security defences.

File No. V-16020/02/2025-INHI (Computer No. 8826346)
Generated from eOffice by SUBHAM SUKUMAR MOHOK, UNDER SECRETARY, DCHAT DEPARTMENT on 29/07/2025 02:48 pm

5. Components of the Design:

Sl. No.	Description
1.	Perimeter Firewall
2.	DC Firewall
3.	Firewall for Remote Sites
4.	Management Console/ Server for Firewalls
5.	Web application firewall + server load balancer +Link load balancer
6.	Security auditing Tool
7.	IAM + PAM for Admin + User Directory
8.	Unified Endpoint Management (UEM)
9.	Endpoint Detection and response (EDR)
10.	Network access control (NAC)
11.	Web Proxy
12.	NG-SIEM Solution including SOAR, UEBA and NDR
13.	DNS, DHCP and IP address management
14.	IT service management (ITSM)
15.	Network management system (NMS)
16.	Zero Trust Network Access for remote users
17.	Secure remote access

Guest WLAN:

Sl. No.	Description
1.	Firewall
2.	Log Server and S/W
3.	DNS, DHCP and IP address management
4.	Web proxy server
5.	WLAN Management including NAC (Network Admission Control)

File No. V-16020/92/2024-INHI (Computer No. [illegible])
Generated from eOffice by [illegible] on 29/07/2025 02:48 pm
526

National Cyber Security Policy -2013

Preamble

1. Cyberspace[1] is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.

2. Owing to the numerous benefits brought about by technological advancements, the cyberspace today is a common pool used by citizens, businesses, critical information infrastructure, military and governments in a manner that makes it difficult to draw clear boundaries among these different groups. The cyberspace is expected to be more complex in the foreseeable future, with many fold increase in networks and devices connected to it.

3. Information Technology (IT) is one of the critical sectors that rides on and resides in cyberspace. It has emerged as one of the most significant growth catalysts for the Indian economy. In addition to fuelling India's economy, this sector is also positively influencing the lives of its people through direct and indirect contribution to the various socio-economic parameters such as employment, standard of living and diversity among others. The sector has played a significant role in transforming India's image to that of a global player in providing world-class technology solutions and IT business services. The government has been a key driver for increased adoption of IT-based products and IT enabled services in Public services (Government to citizen services, citizen identification, public distribution systems), Healthcare (telemedicine, remote consultation, mobile clinics), Education (e-Learning, virtual classrooms, etc) and Financial services (mobile banking / payment gateways), etc. Such initiatives have enabled increased IT adoption in the country through sectoral reforms and National programmes which have led to creation of large scale IT infrastructure with corporate / private participation.

4. In the light of the growth of IT sector in the country, ambitious plans for rapid social transformation & inclusive growth and India's prominent role in the IT global market, providing right kind of focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks, has become one of the compelling priorities for the country. Such a focus enables creation of a suitable cyber security eco-system in the country, in tune with globally networked environment.

[1] ISO / IEC 27032-2012

5. Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation- states and non-state actors. Cyber attacks that target the infrastructure or underlying economic well-being of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures. A cyber related incident of national significance may take any form; an organized cyber attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity. Some of the examples of cyber threats to individuals, businesses and government are identity theft, phishing, social engineering, hactivism, cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates, advanced persistent threats, denial of service, bot nets, supply chain attacks, data leakage, etc. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

6. There are various ongoing activities and programs of the Government to address the cyber security challenges which have significantly contributed to the creation of a platform that is now capable of supporting and sustaining the efforts in securing the cyber space. Due to the dynamic nature of cyberspace, there is now a need for these actions to be unified under a **National Cyber Security Policy**, with an integrated vision and a set of sustained & coordinated strategies for implementation.

7. The cyber security policy is an evolving task and it caters to the whole spectrum of ICT users and providers including home users and small, medium and large enterprises and Government & non-Government entities. It serves as an umbrella framework for defining and guiding the actions related to security of cyberspace. It also enables the individual sectors and organizations in designing appropriate cyber security policies to suit their needs. The policy provides an overview of what it takes to effectively protect information, information systems & networks and also gives an insight into the Government's approach and strategy for protection of cyber space in the country. It also outlines some pointers to enable collaborative working of all key players in public & private to safeguard country's information and information systems. This policy, therefore, aims to create a cyber security framework, which leads to specific actions and programmes to enhance the security posture of country's cyber space.

I. Vision

To build a secure and resilient cyberspace for citizens, businesses and Government

II. Mission

To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

III. Objectives

1) To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.

2) To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).

3) To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.

4) To enhance and create National and Sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.

5) To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources.

6) To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, pilot development, transition, diffusion and commercialisation leading to widespread deployment of secure ICT products / processes in general and specifically for addressing National Security requirements.

7) To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.

Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 29/07/2025 02:48 pm

8) To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.

9) To provide fiscal benefits to businesses for adoption of standard security practices and processes.

10) To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cyber crime or data theft.

11) To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.

12) To create a culture of cyber security and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.

13) To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.

14) To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

IV. Strategies

A. Creating a secure cyber ecosystem

1) To designate a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities.

2) To encourage all organizations, private and public to designate a member of senior management, as Chief Information Security Officer (CISO), responsible for cyber security efforts and initiatives.

3) To encourage all organizations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices. Such policies should include establishing standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

4) To ensure that all organizations earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.

5) To provide fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security.

6) To prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cyber security compliance and proactive actions.

7) To establish a mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts.

8) To encourage entities to adopt guidelines for procurement of trustworthy ICT products and provide for procurement of indigenously manufactured ICT products that have security implications.

B. Creating an assurance framework

1) To promote adoption of global best practices in information security and compliance and thereby enhance cyber security posture.

2) To create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines (Eg. ISO 27001 ISMS certification, IS system audits, Penetration testing / Vulnerability assessment, application security testing, web security testing).

3) To enable implementation of global security best practices in formal risk assessment and risk management processes, business continuity management and cyber crisis management plan by all entities within Government and in critical sectors, to reduce the risk of disruption and improve the security posture.

4) To identify and classify information infrastructure facilities and assets at entity level with respect to risk perception for undertaking commensurate security protection measures.

5) To encourage secure application / software development processes based on global best practices.

6) To create conformity assessment framework for periodic verification of compliance to best practices, standards and guidelines on cyber security.

7) To encourage all entities to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and in networks.

C. Encouraging Open Standards

1) To encourage use of open standards to facilitate interoperability and data exchange among different products or services.

2) To promote a consortium of Government and private sector to enhance the availability of tested and certified IT products based on open standards.

D. Strengthening the Regulatory framework

1) To develop a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space (such as cloud computing, mobile computing, encrypted services and social media) and its harmonization with international frameworks including those related to Internet governance.

2) To mandate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to regulatory framework.

3) To enable, educate and facilitate awareness of the regulatory framework.

E. Creating mechanisms for security threat early warning, vulnerability management and response to security threats

1) To create National level systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

2) To operate a 24x7 National Level Computer Emergency Response Team (CERT-In) to function as a Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management. CERT-In will function as an umbrella organization in enabling creation and operationalization of sectoral CERTs as well as facilitating communication and coordination actions in dealing with cyber crisis situations.

3) To operationalise 24x7 sectoral CERTs for all coordination and communication actions within the respective sectors for effective incidence response & resolution and cyber crisis management.

4) To implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national processes or endangering public safety and security of the Nation, by way of well coordinated, multi disciplinary approach at the National, Sectoral as well as entity levels.

5) To conduct and facilitate regular cyber security drills & exercises at National, sectoral and entity levels to enable assessment of the security posture and level of emergency preparedness in resisting and dealing with cyber security incidents.

F. Securing E-Governance services

1) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan for all e-Governance initiatives in the country, to reduce the risk of disruption and improve the security posture.

2) To encourage wider usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.

3) To engage information security professionals / organisations to assist e-Governance initiatives and ensure conformance to security best practices.

G. Protection and resilience of Critical Information Infrastructure

1) To develop a plan for protection of Critical Information Infrastructure and its integration with business plan at the entity level and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

2) To Operate a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) to function as the nodal agency for critical information infrastructure protection in the country.

3) To facilitate identification, prioritisation, assessment, remediation and protection of critical infrastructure and key resources based on the plan for protection of critical information infrastructure.

4) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan by all critical sector entities, to reduce the risk of disruption and improve the security posture.

5) To encourage and mandate as appropriate, the use of validated and certified IT products.

6) To mandate security audit of critical information infrastructure on a periodic basis.

7) To mandate certification for all security roles right from CISO / CSO to those involved in operation of critical information infrastructure.

8) To mandate secure application / software development process (from design through retirement) based on global best practices.

H. Promotion of Research & Development in cyber security

1) To undertake Research & Development programs for addressing all aspects of development aimed at short term, medium term and long term goals. The Research & Development programs shall address all aspects including development of trustworthy systems, their testing, deployment and maintenance throughout the life cycle and include R&D on cutting edge security technologies.

2) To encourage Research & Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of cyber security challenges and target for export markets.

3) To facilitate transition, diffusion and commercialisation of the outputs of Research & Development into commercial products and services for use in public and private sectors.

4) To set up Centres of Excellence in areas of strategic importance for the point of security of cyber space.

5) To collaborate in joint Research & Development projects with industry and academia in frontline technologies and solution oriented research.

I. Reducing supply chain risks

1) To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices.

2) To build trusted relationships with product / system vendors and service providers for improving end-to-end supply chain security visibility.

3) To create awareness of the threats, vulnerabilities and consequences of breach of security among entities for managing supply chain risks related to IT (products, systems or services) procurement.

J. Human Resource Development

1) To foster education and training programs both in formal and informal sectors to support the Nation's cyber security needs and build capacity.

2) To establish cyber security training infrastructure across the country by way of public private partnership arrangements.

3) To establish cyber security concept labs for awareness and skill development in key areas.

4) To establish institutional mechanisms for capacity building for Law Enforcement Agencies.

K. Creating Cyber Security Awareness

1) To promote and launch a comprehensive national awareness program on security of cyberspace.

2) To sustain security literacy awareness and publicity campaign through electronic media to help citizens to be aware of the challenges of cyber security.

3) To conduct, support and enable cyber security workshops / seminars and certifications.

L. Developing effective Public Private Partnerships

1) To facilitate collaboration and cooperation among stakeholder entities including private sector, in the area of cyber security in general and protection of critical information infrastructure in particular for actions related to cyber threats, vulnerabilities, breaches, potential protective measures, and adoption of best practices.

2) To create models for collaborations and engagement with all relevant stakeholders.

3) To create a think tank for cyber security policy inputs, discussion and deliberations.

M. Information sharing and cooperation

1) To develop bilateral and multi-lateral relationships in the area of cyber security with other countries.

2) To enhance National and global cooperation among security agencies, CERTs, Defence agencies and forces, Law Enforcement Agencies and the judicial systems.

3) To create mechanisms for dialogue related to technical and operational aspects with industry in order to facilitate efforts in recovery and resilience of systems including critical information infrastructure.

N. Prioritized approach for implementation

To adopt a prioritized approach to implement the policy so as to address the most critical areas in the first instance.

V. Operationalisation of the Policy

This policy shall be operationalised by way of detailed guidelines and plans of action at various levels such as national, sectoral, state, ministry, department and enterprise, as may be appropriate, to address the challenging requirements of security of the cyberspace.

Cybersecurity "Defence In Depth" Strategy for Protecting Critical Health Information Systems

Office of Advisor (Cyber) – OAC

1 Introduction and Threat Landscape

The healthcare sector faces unprecedented cybersecurity challenges with increasing digitization of medical records, proliferation of Internet of Medical Things (IoMT) devices, and growing sophistication of cyber threats. Additionally, this sector has become a primary target for cybercriminals due to the high value of Protected Health Information (PHI) and the critical nature of medical services.

This document presents a comprehensive Defence in Depth cybersecurity framework specifically tailored for critical healthcare organizations, addressing the unique requirements of protecting Protected Health Information (PHI), ensuring patient safety, and maintaining operational continuity of critical medical services.

1.1. Trends in Healthcare

- **Ransomware attacks** targeting Hospital Information Systems (HIS) and Electronic Health Records (EHR)
- **Medical device vulnerabilities** in connected infusion pumps, ventilators, and cardiac monitors
- **Data breaches** affecting Electronic Protected Health Information (ePHI)
- **Supply chain attacks** targeting Health Information Management Systems (HIMS)
- **Insider threats** compromising Patient Health Information access controls

1.2. Unique Healthcare Security Requirements

Healthcare cybersecurity differs from traditional enterprise security due to:

- **Patient Safety Priority**: Security measures must never compromise patient care delivery
- **Regulatory Compliance**: Until National Standards are formulated, International best practices and guidelines may be followed such as HIPAA Security Rule, FDA Medical Device Reporting (MDR) requirements
- **Legacy Systems Integration**: Many healthcare facilities operate aging Picture Archiving and Communication Systems (PACS)
- **24x7 Operations**: Critical care systems require continuous availability
- **Diverse Stakeholder Ecosystem**: Integration with Laboratory Information Systems (LIS), Radiology Information Systems (RIS), and Pharmacy Information Systems

1.3. Key Recommendations

- Implementation of layered security controls across distinct security domains
- Establishment of specialized healthcare cybersecurity governance aligned with regulatory requirements

File No. V-16020/63/2025-INI-I (Computer No. 8386793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 28/07/2025 08:49 pm
536

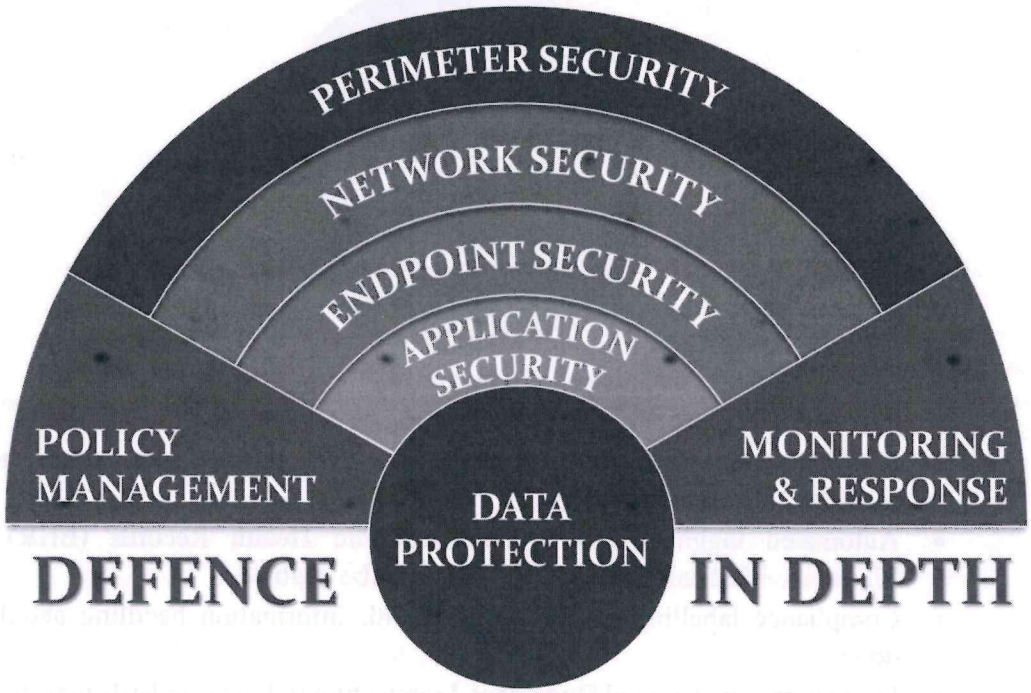
- Deployment of medical device-specific security measures
- Creation of 24x7 healthcare-focused Security Operations Centres (SOCs)
- Development of incident response capabilities prioritizing patient safety
- Formulation of National Standards and following of prevalent international standards until national standards are formed

1.4. Expected Outcomes

- Enhanced protection of Electronic Health Records (EHR) and Electronic Medical Records (EMR)
- Improved alignment with healthcare cyber best practices across the world (like HIPAA, FDA guidelines)
- Reduced risk of ransomware attacks disrupting patient care
- Strengthened security for Picture Archiving and Communication Systems (PACS)
- Protected Internet of Medical Things (IoMT) infrastructure

File No. V-16020/63/2025-INI-I (Computer No. 4386793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 28/07/2025 08:49 pm

2 Defence in Depth Architecture



2.1. Strategic Framework Overview

The Defence in Depth strategy implements seven concentric layers of security controls, each designed to protect healthcare-specific assets and address sector-unique threats. This layered approach ensures that if one security control fails, multiple additional layers continue protecting critical healthcare data and systems.

2.2. Core Principles

- **Redundancy**: Multiple overlapping security controls protect the same assets
- **Diversity**: Different types of security technologies prevent single points of failure
- **Depth**: Security controls span from perimeter to core data protection
- **Healthcare Focus**: All controls specifically address medical industry requirements
- **Regulatory Alignment**: Controls support Global and healthcare compliance needs

File No. V-16020/53/2025-INI-I (Computer No. 8286793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 28/07/2025 08:49 pm
538

2.3. Defence in Depth

2.3.1. Layer 1- DATA PROTECTION



2.3.1.1. Data Classification and Governance

- Risk-Based Categorization of Data should be documented
- Classify patient data by sensitivity levels: PHI, genetic data, mental health records, substance abuse records
- Automated tagging systems for Electronic Health Records (EHR) and Electronic Medical Records (EMR) should be enabled
- Compliance labelling for Protected Health Information handling should be done
- Integration with Clinical Document Architecture (CDA) standards may be done

2.3.1.2. File Integrity Monitoring (FIM)

- Real-time detection of unauthorized changes to EHR databases and medical images
- Monitoring of Picture Archiving and Communication Systems (PACS) for tampering detection
- Audit log integrity verification for compliance reporting
- Configuration monitoring for medical device settings and parameters

2.3.1.3. Data Backup

- Immutable Backup Systems must be implemented
- Implement Write-Once-Read-Many (WORM) technologies for patient records
- Ransomware-resistant storage protecting critical medical data must be deployed
- Disaster recovery capabilities to be put in place ensuring patient data availability during emergencies

2.3.1.4. Secure Data Destruction

- Compliant purging of patient records per regulatory retention policies should be carried out
- Secure decommissioning of medical devices containing PHI should be undertaken
- Media sanitization for hard drives and storage devices should be done
- Certificate of destruction documentation for audit requirements must be produced

2.3.1.5. Encryption of Data in Transit

File No. V-16020/83/2025-INI-I (Computer No. 8286793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 29/07/2025 08:49 pm
539

- Encrypt HL7 FHIR messages between healthcare systems and Health Information Exchange (HIE) networks
- Secure telemedicine sessions and remote patient monitoring communications
- Protect laboratory results transmission and mobile health application data
- Clinical Document Architecture (CDA) exchange encryption must be implemented

2.3.1.6. Data at Rest Protection

- Database encryption for stored patient records and medical histories
- Medical image encryption in PACS systems and Vendor Neutral Archives (VNA)
- Genomic data protection implementation for research and clinical genetics programs
- Internet of Medical Things (IoMT) device storage encryption for connected medical equipment must be implemented

2.3.1.7. Identity and Access Management

- Provider credentialing and patient identity matching systems to be implemented
- Access must be federated across hospital networks and partner organizations
- Integration with Master Patient Index (MPI) systems should be carried out
- Healthcare Common Procedure Coding System (HCPCS) access controls should be implemented

2.3.1.8. Dynamic Access Management

- Role-based permissions ensuring clinical staff access relevant patient data only
- Privileged Access Management with break-glass emergency procedures for patient care
- Secure access to be implementation for EHRs, prescription systems, and remote healthcare applications
- Zero Trust Identity with behavioural analytics and device trust assessment
- Just-in-Time Access for emergency care, specialist consultations, and research projects

File No. V-16020/63/2025-INI-I (Computer No. 8286793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 29/07/2025 08:49 pm
540

2.3.2. Layer 2: APPLICATION SECURITY



2.3.2.1. **Healthcare Application Firewall** Implementation is equally important to be implemented as the network firewall

2.3.2.2. Web Application and API Protection

- Protect Electronic Health Record (EHR) systems and Electronic Medical Record (EMR) databases from SQL injection attacks
- Secure Patient Health Information (PHI) portals from application-layer threats
- HL7 FHIR API security with OAuth authentication for healthcare interoperability standards
- Clinical Document Architecture (CDA) exchange protection

2.3.2.3. Picture Archiving and Communication Systems Protection

- Secure PACS against unauthorized access to diagnostic imaging data
- Protect radiological workflows and medical imaging databases
- Implement DICOM (Digital Imaging and Communications in Medicine) protocol security
- Tele-radiology system protection and Vendor Neutral Archive (VNA) security should be ensured

2.3.2.4. Static and Dynamic Analysis

- Static Application Security Testing (SAST) for Laboratory Information Systems (LIS), Radiology Information Systems (RIS), and Anatomic Pathology Laboratory Information Systems (APLIS) should be mandated
- DAST for Hospital Information Systems (HIS), Computerized Provider Order Entry (CPOE), and Clinical Decision Support Systems (CDSS) should be carried out
- Continuous and periodic security testing of healthcare application portfolios should be carried out

2.3.2.5. Internet of Medical Things (IoMT) Protection

- Secure infusion pumps, ventilators, cardiac monitors, and implantable medical devices
- Follow FDA cybersecurity premarket guidance and post-market surveillance requirements

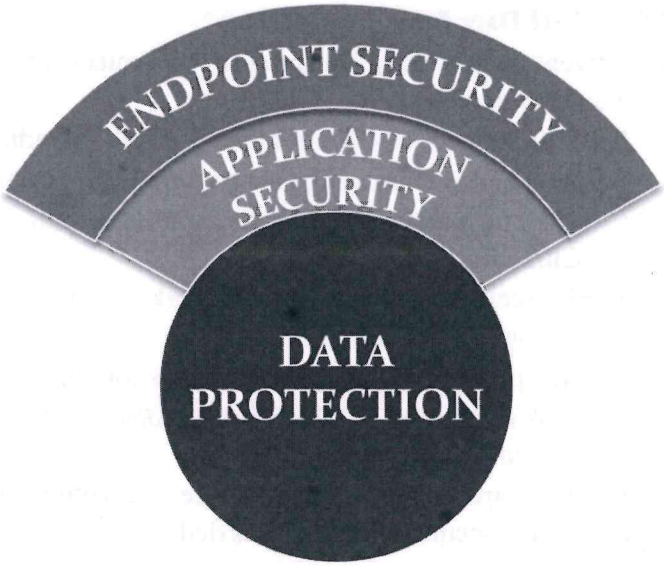
File No. V-16020/53/2025-INI-I (Computer No. 8386793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 29/07/2025 08:49 pm

- Protect web-based device management consoles and remote monitoring applications
- Medical device application interface security for critical care equipment

2.3.2.6. Healthcare System Interoperability and clinical integration security

- Container security for clinical micro-services and telemedicine platforms should be implemented
- Remote patient monitoring system protection and mHealth application security should be implemented
- Master Patient Index (MPI) system security and Admission Discharge Transfer (ADT) interface protection should be carried out
- Software Composition Analysis for third-party libraries in Health Information Management Systems (HIMS) should be done

2.3.3. Layer 3: ENDPOINT SECURITY



2.3.3.1. Medical Workstation Security

- Isolate clinical workstations accessing EHR/EMR systems from administrative networks
- PACS workstation firewalls should prevent lateral movement to Hospital Information Systems (HIS)
- Host-based intrusion detection on EHR access points and clinical decision support terminals must be deployed

2.3.3.2. IoMT Device Updates

- Coordinate security updates for infusion pumps, ventilators, MRI systems, and CT scanners
- Follow global guidelines such as FDA Medical Device Reporting (MDR) guidelines for security patches
- Manage patches for Laboratory Information Systems (LIS) and Radiology Information Systems (RIS)
- Maintain clinical workflow continuity during security updates

2.3.3.3. Clinical Endpoint Monitoring

File No. V-16020/53/2025-INI-I (Computer No. 8286793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 28/07/2025 08:49 pm

- Mandatorily deploy EDR on workstations accessing Electronic Protected Health Information (ePHI)
- Behavioural analysis for breach detection and compliance reporting
- Monitor Internet of Medical Things (IoMT) endpoints for unauthorized access attempts
- Anomaly detection for patient care device security incidents

2.3.3.4. Medical Equipment Assessment

- Continuous scanning of connected medical equipment should be carried out
- Clinical application vulnerability tracking in Health Information Management Systems (HIMS) should be implemented
- Telemedicine platform and remote patient monitoring system vulnerability management should be implemented
- Post-market surveillance requirements for medical device cybersecurity should be done

2.3.3.5. PHI Data Loss Prevention

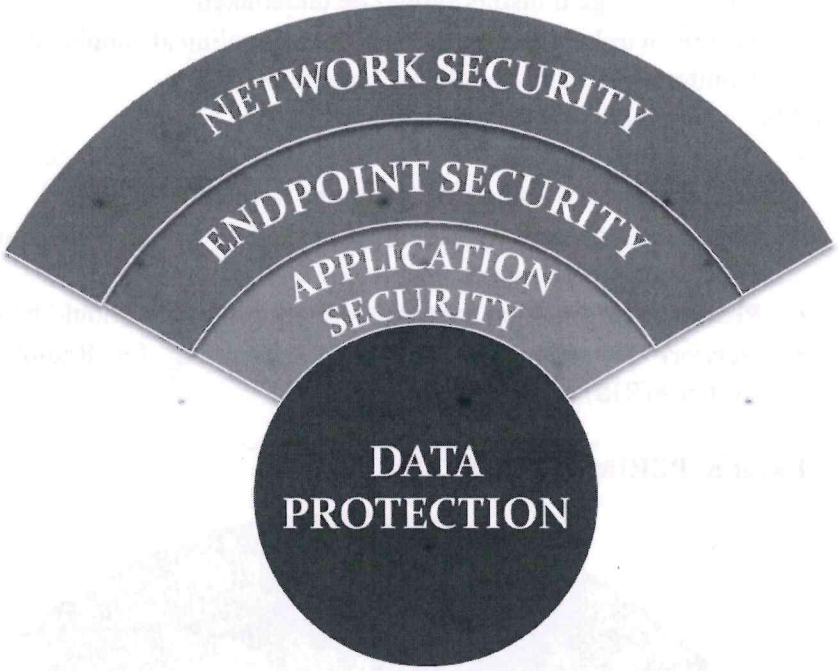
- Prevent unauthorized transmission of Protected Health Information via email and USB devices
- Medical image protection for DICOM files on radiology workstations
- Secure diagnostic imaging data on mobile diagnostic units
- Cloud storage access controls for clinical endpoints should be implemented

2.3.3.6. Clinical System Security

- Apply security benchmarks to workstations running PACS viewers and Electronic Health Record systems
- Secure operating system configurations for embedded medical device systems
- Full disk encryption on tablets and laptops used for bedside EMR access should be enabled
- Point-of-care documentation device encryption and ambulatory monitoring equipment security should be carried out

File No. V-16020/87/2025-INI-I (Computer No. 8286793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 28/07/2025 08:49 pm
543

2.3.4. Layer 4: NETWORK SECURITY



2.3.4.1. Clinical Network Architecture

- Isolate Electronic Health Record (EHR) networks from administrative systems
- Separate Protected Health Information (PHI) traffic from general hospital operations
- Segment Internet of Medical Things (IoMT) devices including infusion pumps, ventilators, and cardiac monitors
- Isolate medical devices from Hospital Information Systems (HIS) networks

2.3.4.2. Healthcare Zero Trust Architecture

- Continuous verification of network access to Picture Archiving and Communication Systems (PACS)
- Laboratory Information Systems (LIS) and Electronic Medical Record (EMR) database protection should be used
- Micro-segmentation for Computerized Provider Order Entry (CPOE) and Clinical Decision Support Systems (CDSS) should be done
- Least-privilege access principles for clinical systems should be followed

2.3.4.3. Medical Device Network Control

- Control network access for diagnostic equipment, patient monitors, and medical imaging systems
- Device identity verification and health status assessment should be carried out
- Multi-factor authentication for telemedicine consultations and remote ePHI access should be implemented
- Health Information Exchange (HIE) connection security should be ensured

2.3.4.4. Clinical Communication Protection

- VoIP security for operating rooms, nurse call systems, and physician consultation platforms should be ensured

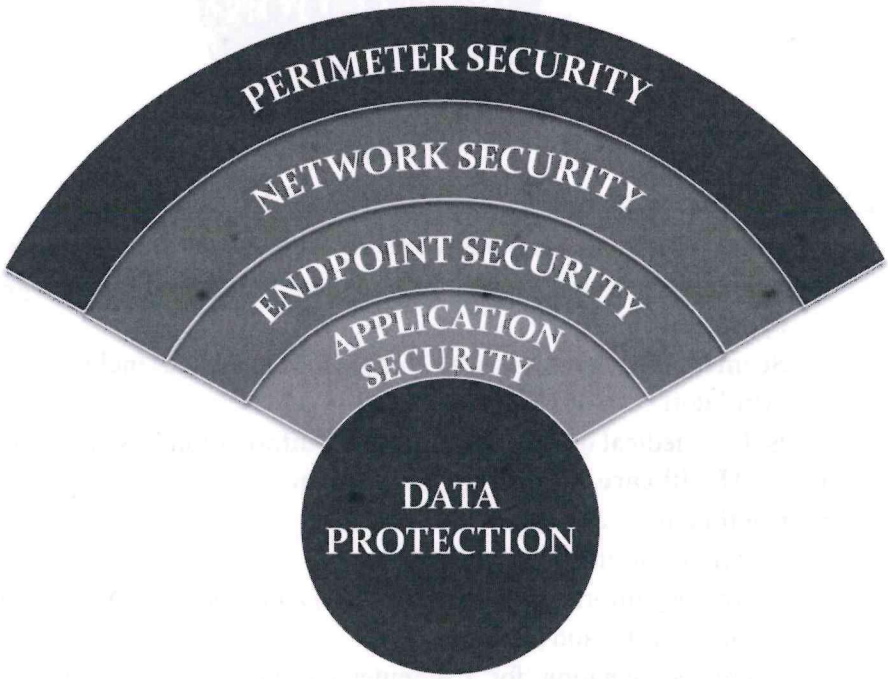
File No. V-16020/53/2025-INI-I (Computer No. 8386793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 29/07/2025 08:49 pm
544

- Encrypted medical data transmission protecting HL7 FHIR messages and DICOM image transfers should be undertaken
- Secure wireless networks for mobile clinical applications and bedside monitoring systems should be implemented

2.3.4.5. Network Traffic Management

- Application content filtering blocking unauthorized access from clinical workstations accessing PHI should be implemented
- Data center firewall management protecting Master Patient Index (MPI) and HIMS systems should be enabled
- Pharmacy Information Systems network protection should be implemented
- Network Detection and Response monitoring for Radiology Information Systems (RIS) access should be ensured

2.3.5. Layer 5: PERIMETER SECURITY



2.3.5.1. Healthcare Network Perimeter Defense

- Deep packet inspection of HL7 FHIR traffic and Electronic Health Record (EHR) communications should be carried out
- Health Information Exchange (HIE) connection filtering entering hospital networks should be implemented
- Application-aware filtering of Internet of Medical Things (IoMT) communications should be done
- Medical device traffic filtering for infusion pumps, ventilators, and diagnostic imaging systems should be done

2.3.5.2. Clinical System Attack Prevention

- Real-time blocking of malicious attempts targeting Picture Archiving and Communication Systems (PACS) should be done

File No. V-16020/87/2025-INI-I (Computer No. 8386733)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 29/07/2025 08:49 pm

- Laboratory Information Systems (LIS) and Electronic Medical Record (EMR) database protection should be deployed
- Medical device exploitation detection and Patient Health Information (PHI) exfiltration prevention should be implemented
- Connected medical equipment vulnerability monitoring should be ensured

2.3.5.3. Healthcare DMZ Implementation

- Isolate patient portals and telemedicine platforms from internal clinical networks
- Health Information Management Systems (HIMS) web interface protection should be implemented
- Medical device remote access zones for vendor maintenance of MRI systems and CT scanners should be used
- Critical care monitoring equipment secure access zones should be created

2.3.5.4. Protected Health Information Monitoring

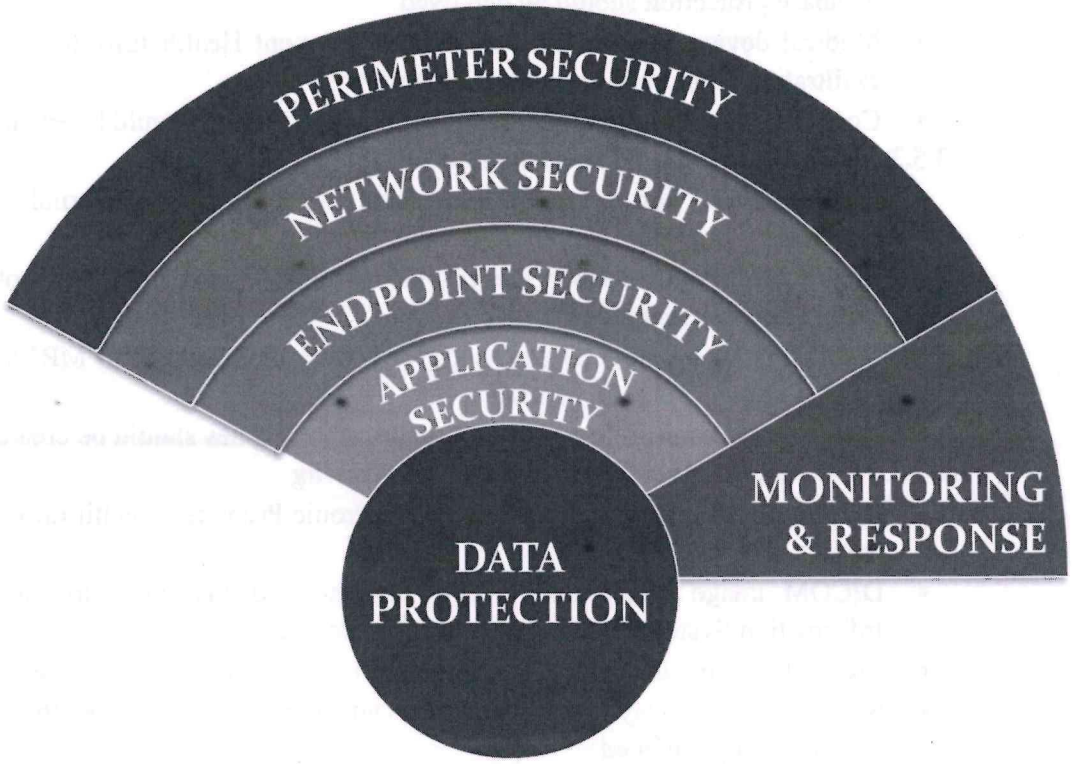
- Prevent unauthorized transmission of Electronic Protected Health Information (ePHI)
- DICOM image protection blocking unauthorized sharing from Radiology Information Systems (RIS) should be implemented
- Medical imaging data and diagnostic report security should be ensured
- Secure email gateway filtering malicious attachments targeting healthcare staff should be implemented

2.3.5.5. Clinical System Continuity

- DDoS prevention should be deployed ensuring continuous access to Computerized Provider Order Entry (CPOE) systems
- Clinical Decision Support Systems (CDSS) availability during cyber attacks must be ensured
- Physician-to-physician consultation protection containing Patient Health Information should be ensured
- Healthcare communication platform security should be ensured

File No. V-16020/53/2025-INI-I (Computer No. 8286793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 29/07/2025 08:49 pm
546

2.3.6. Layer 6: MONITORING AND RESPONSE



2.3.6.1. Medical-Specific Threat Intelligence

- Monitor emerging threats targeting Electronic Health Record (EHR) systems and ransomware campaigns
- Internet of Medical Things (IoMT) device vulnerability intelligence from global and national advisories should be collated and corelated
- ICS-CERT alerts for medical device security threats should be closely monitored
- Healthcare-focused threat intelligence feeds and industry collaboration should be done

2.3.6.2. Medical Cyber Security Operations Center

- Continuous surveillance of Electronic Protected Health Information (ePHI) access patterns should be done
- Medical device network traffic monitoring and Electronic Medical Record (EMR) system availability should be ensured
- Clinical escalation protocols and playbooks for incidents affecting patient care systems should be set-up
- Computerized Provider Order Entry (CPOE) and Clinical Decision Support Systems (CDSS) monitoring should be ensured

2.3.6.3. Healthcare Incident Response

- Immediate detection and containment of breaches affecting Protected Health Information (PHI) should be ensured
- Clinical situational awareness during security events should be ensured

File No. V-16020/63/2025-INI-I (Computer No. 8386793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 28/07/2025 08:49 pm

- Hospital operations and Health Information Management Systems (HIMS) performance monitoring should be mandated

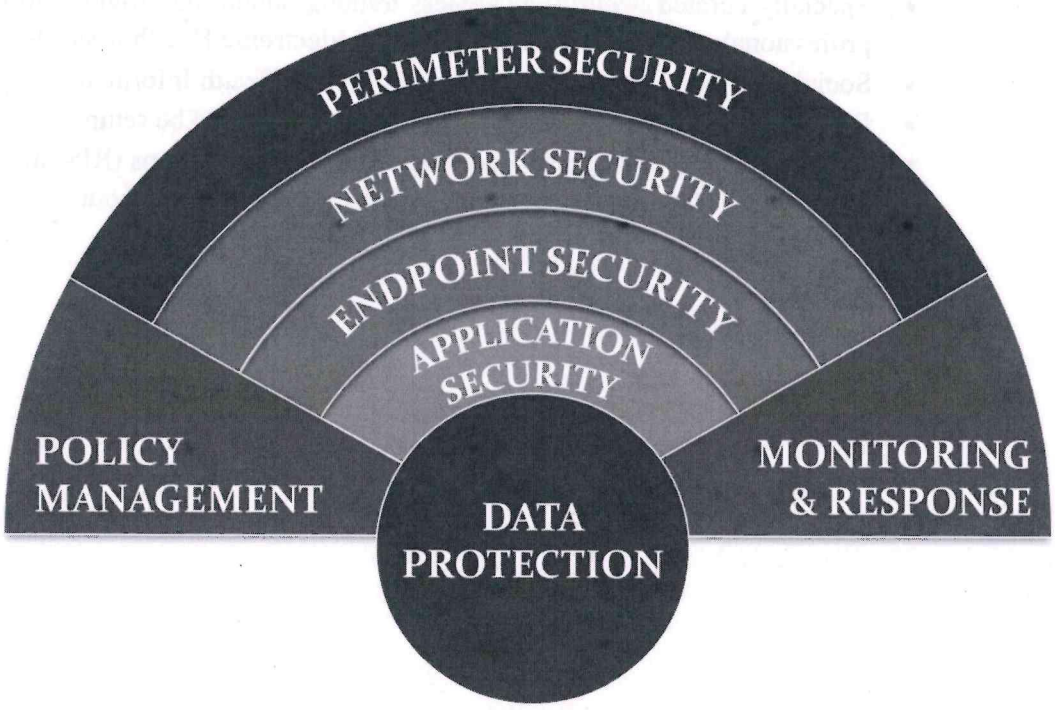
2.3.6.4. Healthcare SIEM Implementation

- Centralized logging and correlation of security events from Radiology Information Systems (RIS) should be done
- Pharmacy Information Systems and Master Patient Index (MPI) database monitoring should be done
- Security Orchestration, Automation and Response (SOAR) for clinical environments with automated response workflows should be implemented
- Medical device quarantine and Electronic Health Record system isolation capabilities should be created

2.3.6.5. Healthcare Personnel Monitoring

- UEBA for clinical staff accessing Patient Health Information should be setup
- Anomalous pattern detection in EHR usage and medical device interactions should be monitored
- Medical device vulnerability management following cybersecurity best practices should be ensured
- Continuous assessment of connected medical equipment per Medical Device Reporting (MDR) requirements should be done

2.3.7. Layer 7: POLICY MANAGEMENT



2.3.7.1. Indian Healthcare Data Protection Framework Integration

- Implement Digital Personal Data Protection Act (DPDP) 2023 compliance for Electronic Health Records (EHR)
- Patient Health Information (PHI) protection aligned with Ministry of Health and Family Welfare guidelines

File No. V-16020/53/2025-INI-I (Computer No. 8286793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 29/07/2025 08:49 pm

- Ayushman Bharat Digital Mission (ABDM) security framework integration
- Health ID management and secure interoperability across Hospital Information Systems (HIS)

2.3.7.2. Healthcare Cybersecurity Governance

- Align policies with National Digital Health Mission (NDHM) standards
- Indian Medical Council regulations for telemedicine and digital health platforms to be followed
- Security architecture for Picture Archiving and Communication Systems (PACS) should be defined
- Laboratory Information Systems (LIS) and Clinical Decision Support Systems (CDSS) compliance to security best practices should be ensured

2.3.7.3. Healthcare-Specific Risk Assessment

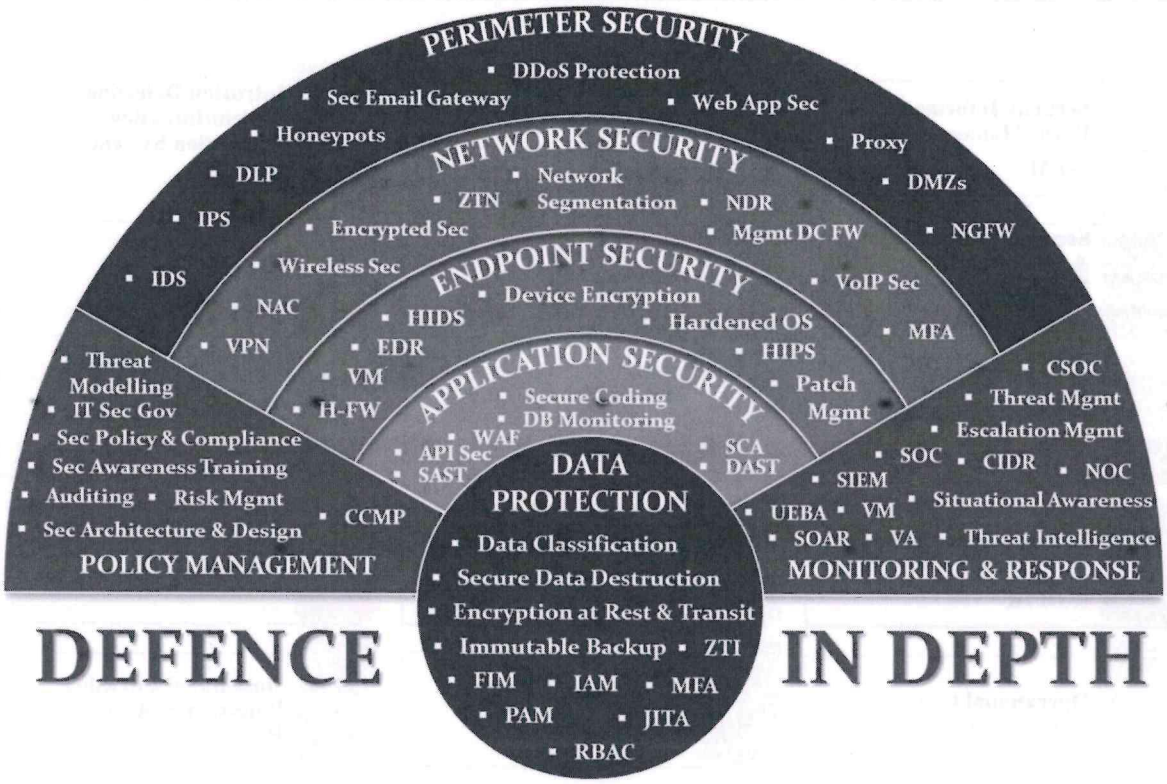
- Risk analysis for Internet of Medical Things (IoMT) devices and Electronic Protected Health Information (ePHI) should be carried out
- Health Information Exchange (HIE) vulnerability assessment in Indian healthcare context should be done
- Cyber Crisis Management Plan including ransomware attacks on Computerized Provider Order Entry (CPOE) systems should be formulated
- Coordination with Indian Computer Emergency Response Team (CERT-In) and state health authorities

2.3.7.4. Healthcare Security Program

- Specially curated Security awareness training should be provided to medical professionals on phishing threats targeting Electronic Health Records
- Social engineering attack prevention for Patient Health Information access
- DICOM imaging data secure handling protocols should be setup
- Regular security auditing of Radiology Information Systems (RIS) and Health Information Management Systems (HIMS) should be carried out

File No. V-16020/83/2025-INI-I (Computer No. 8386793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 29/07/2025 08:49 pm

2.4. IMPLEMENTATION STRATEGY



2.4.1. The implementation of the Defence in Depth can be done in a phased manner:

2.4.1.1. Phase 1: Foundation (Months 1-6)

- Establish data classification and encryption frameworks
- Deploy basic endpoint protection on clinical workstations
- Implement network segmentation for critical systems
- Set up initial monitoring and incident response capabilities

2.4.1.2. Phase 2: Enhancement (Months 7-12)

- Deploy advanced application security controls
- Implement comprehensive medical device security
- Establish 24x7 healthcare Cyber Security Operations Centre (CSOC) operations
- Complete perimeter security deployment

2.4.1.3. Phase 3: Optimization (Months 13-18)

- Deploy advanced analytics and behavioural monitoring
- Implement zero trust architecture
- Complete policy and governance framework
- Conduct comprehensive security assessments

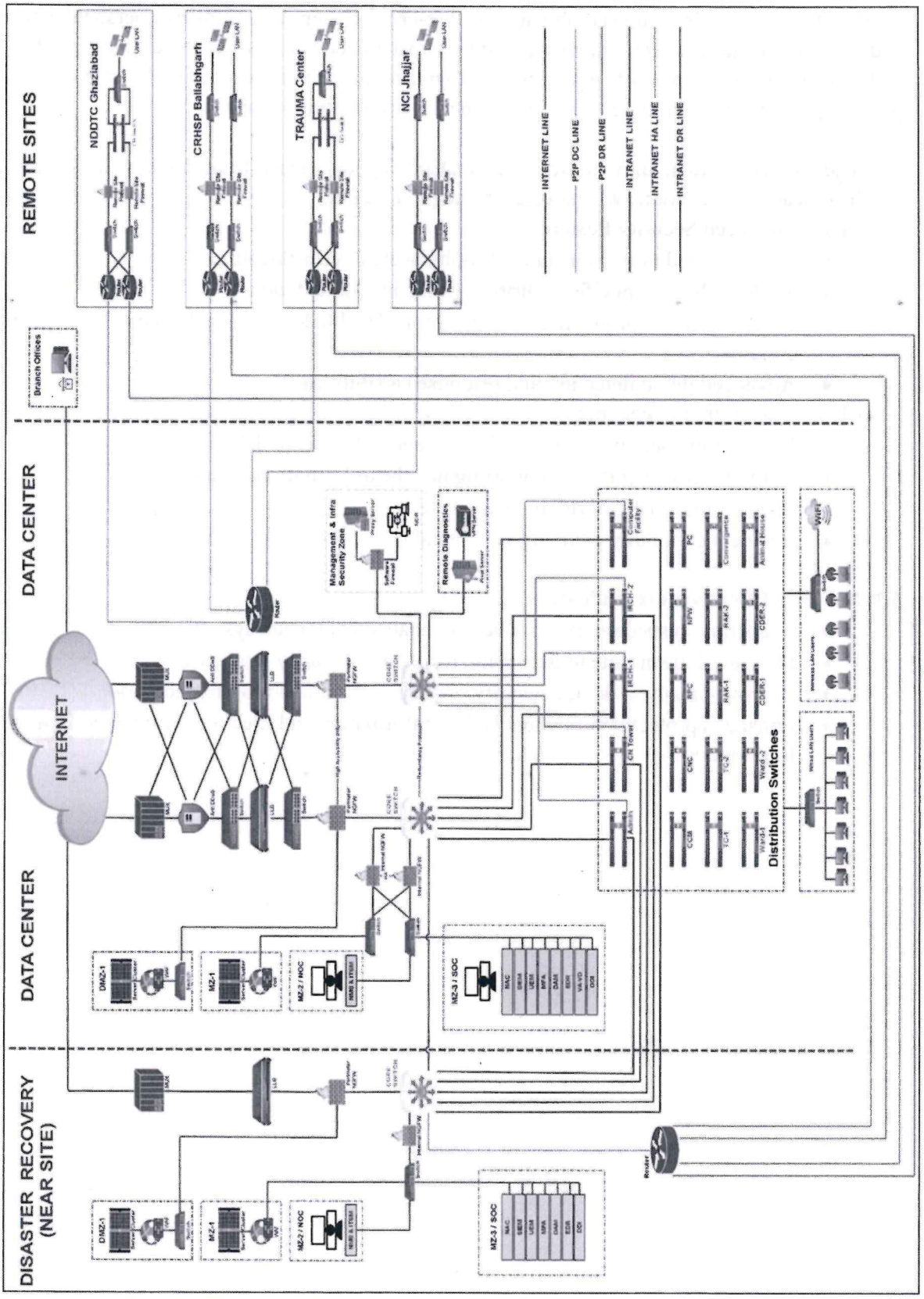
File No. V-16020/83/2025-INI-I (Computer No. 8286793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 29/07/2025 08:49 pm
550

3 Model Technical Implementation Stack



File No. V-16020/83/2025-INI-I (Computer No. 83867933)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 29/07/2025 08:49 pm

4 Model Network Architecture



File No. V-16020/63/2025-INI-I (Computer No. 8286793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 29/07/2025 08:49 pm

5 Conclusion

The healthcare sector's unique combination of life-critical operations, sensitive personal data, and complex regulatory requirements demands a specialized approach to cybersecurity. This Defence in Depth framework provides a comprehensive, healthcare-focused strategy that protects patient safety while securing critical health information systems.

3.1. The implementation of this Defence in Depth cybersecurity framework will provide healthcare organizations with several **strategic benefits**:

3.1.1. Enhanced Security Posture

- Multi-layered protection against sophisticated cyber threats
- Medical device-specific security controls implementation
- Comprehensive protection for Electronic Health Records and medical imaging systems
- Advanced threat detection and response capabilities

3.1.2. Operational Excellence

- Minimal impact on clinical workflows and patient care delivery
- 24x7 security operations supporting healthcare's continuous operations
- Incident response prioritizing patient safety
- Business continuity planning for critical medical service

3.2. Security Effectiveness Indicators

- Reduction in successful cyber-attacks against healthcare systems
- Decreased mean time to detect and respond to security incidents
- Improved medical device security posture and vulnerability remediation
- Enhanced protection of Patient Health Information and Electronic Protected Health Information

File No. V-16020/83/2025-INI-I (Computer No. 8386793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 28/07/2025 08:49 pm
553

Appendix
(Reference Para 2 of NSCS ID No
46/87/2025-NSCS(CS)
dated 07 May 2025)

SOP FOR CRITICAL SECTOR ENTITIES

Introduction

1. The security situation in view of the recent terrorist attack on Indian Tourists at Pehalgam and consequent Indian response through Operation Sindoor continuous to be complex and needs to be closely monitored by all stakeholders. Cyberspace has also seen an increased activity and threats from Pakistan and other adversarial elements. Threat actors from Pakistan in association with her partners may cause disruption/ degradation of our essential services being provisioned through digital infrastructure. Therefore, our critical sectors (both Public and Private) need to be prepared to ensure strong defences.

Aim

2. The aim of this SOP is to highlight certain measures to be adopted by Critical Sectors to safeguard Indian Cyberspace.

Actions for Immediate Implementation

3. **Action on Alerts & Advisories**. All stakeholders to give high priority to all alerts & advisories issued by NCIIPC / CERT-In/Int Agencies/ Sector Regulators. All applicable Action Taken Reports to be forwarded on time as per laid down procedures. Ensure all internal sensitive policies, procedures, baselines and guidelines have been updated and are being followed on ground.

4. **24 x 7 Monitoring**. All stakeholders to advise respective entities under their jurisdiction to switch to heightened alert mode with 24 X 7 SOC and NOC operations monitoring. Ensure near 100% manpower availability and high state of readiness for proactive threat detection and mitigation. Regularly examine logs of web servers, perimeter devices (like WAF, Firewall DNS) to detect malicious request/ traffic. Focus to maintain serviceability of critical services of respective entities.

File No. V-16020/83/2025-INI-I (Computer No. 8286793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 28/07/2025 05:40 pm

5. **Monitoring of Privileged Accounts**. All privilege accounts be immediately audited to detect any unauthorised privileges/ unjustified privilege creep/ unauthorized access. Least privilege policy be ensured for such accounts.

6. **Backup Critical Data**. Offline, encrypted backups of all critical Information infrastructure and business-critical assets be maintained. Store geographically dispersed copies. Carry out checks to ensure capability to recover operations from backup.

7. **Reporting of Incidents**. All cyber incidents to be reported as per directions of CERT-In and NCIIPC.

8. **Activation of Incident Response Plan**. IR teams should be in readiness to respond to any cyber incident, maintain continuous connect with NCIIPC / CERT-In, and connect up with any prior incident reporting done with CERT-In / NCIIPC/ Sector Regulators.

9. **Patch Management**. Keep all applications / OS / hardware updated. Patch management of vulnerabilities be carried out regularly on priority. Emergency patches, if any may also be checked for serviceability of the applicable ecosystem before deployment.

10. **Threat Hunting**. Proactive threat hunting to be carried out to rule out any compromise or persistence of threat actors in systems. Sector Regulators to keep respective sectors updated with regard to sector wise applicable threats.

11. **Managed Service Providers (MSPs)/ Vendors on High Level of Alertness**. Sensitize MSPs/Vendors providing third party security tools/ services to maintain high level of alertness with regard to the current situation. All organisations/ entities to maintain extra vigil over such service providers, particularly with regard to Quality of Services and response times. Ensure adherence to the Cyber Security Practices and deployment of high-quality manpower and standby teams required in case of response.

12. **Access Controls**. Enforce MFA across all accounts wherever feasible and disable non-essential user access and third-party integrations.

13. **DDoS Mitigation and Website Defacement**. Web facing information infrastructure including web portal/ websites must be guarded against DDoS attack by implementing proper DDoS mitigation tools. Geo Fencing be implemented keeping business requirements in mind. Special monitoring to be carried out to detect website defacements, if any.

14. **Special Watch on Phishing and Social Engineering**. Monitor e-mails for any phishing attacks. Report all phishing e-mails. Vigilance / reporting of phishing websites be carried out. Conduct awareness sessions about social engineering principles. Official work-related activities not to be shared through social media.

15. **Employee Sensitization and Monitoring**. Employees be sensitised to be alert and report any phishing, credential theft or attempt on organizational systems. Employees to be encouraged to report inadvertent cyber hygiene breaches. Carry out proper screening and verification of out sourced/ third party employees working in respective organisations for outsourced services.

16. **Cyber Drills**. Test the effectiveness of the Incident Response Plan (IRP) / CCMP by conducting cyber drills, especially against ransomware/ DDoS attacks. Gaps identified during the drills be used to update CCMP.

17. **Attack Surface Management and Vulnerability Assessment**. Regular VA scanning of IT ecosystem including the networks for finding security gaps, if any. Same to be carried out regularly for internal or third-party services. Continuous red teaming be carried out to find out Vulnerabilities & plug them before exploitation by threat actor.

18. **Redundancy Activation**. High availability of critical assets/services to be ensured for business continuity in case of any contingency.

19. **Email**. All entities to use only official emailing infrastructure for communications. No commercial/ private email services to be used.

20. **Physical Security**. All entities to maintain full alertness with regards to physical security of their assets.

File No. V-16020/83/2025-INI-I (Computer No. 8286733)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 28/07/2025 03:30 pm

21. **Risk Management**. All entities to carry out fresh Risk Assessment, Threat Modelling and Business Impact Analysis in view of the current geo-political scenario. Stakeholders to review Supply Chain Risk Management afresh in light of the current situation. National Cybersecurity Reference Framework may also be referred to in this regard.

22. **Domain Monitoring**. Lay special emphasis on Brand Reputation monitoring and creation of similar sounding/ linked malicious domains.

23. **Cloud Service Providers**. Review arrangements with Cloud Service Providers and ensure that adequate security controls have been built into the arrangement.

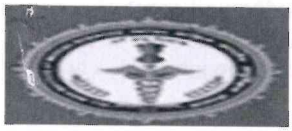
24. **Data**. Data Owners and Data Custodians within organisations to review roles and assets under charge so as to ensure security.

25. **Encryption**. All cryptographic arrangements with respect to handling of data to be monitored closely and implementation ensured.

Conclusion

26. Following the above-mentioned measures will ensure a strong cyber security posture for all critical sectors. This needs to be followed in letter and spirit, however, all existing orders will remain in vogue.

File No. V-16020/83/2025-INI-I (Computer No. 8386793)
Generated from eOffice by SUBHANSHU KUMAR, ASO(SK)-PMSSY-I-MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 29/07/2025 03:30 pm



Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: : Framing of Regulation under the AIIMS Act, 1956 as amended by the Act of 2012.

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Wed, Dec 17, 2025 at 3:15 PM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **Director .** <director@aiimspatna.org>
Date: Tue, Aug 12, 2025 at 12:43 PM
Subject: Fwd: : Framing of Regulation under the AIIMS Act, 1956 as amended by the Act of 2012.
To: DDA AIIMS PATNA <dda@aiimspatna.org>
Cc: SAURABH VARSHNEY <drsaurabh68@gmail.com>

Sd/-
Prof. (Dr.) Saurabh Varshney
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109

---------- Forwarded message ---------
From: **pmssysection iv** <pmssysectioniv@gmail.com>
Date: Tue, Aug 12, 2025 at 10:23 AM
Subject: : Framing of Regulation under the AIIMS Act, 1956 as amended by the Act of 2012.
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, <madhabananda@gmail.com>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, <drppjoshi@aiimsnagpur.edu.in>, Executive Director Raebareli <edaiimsrbl@gmail.com>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, Sharma, DN <sharmadn@aiims.edu>, Dr.Shakti kumar Gupta <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, <sachimohanty@rediffmail.in>
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, Dy Director Administration AIIMS, Raebareli <ddaaiimsrbl@gmail.com>, Dr. Pradip Kumar <kpradip10@gmail.com>, <dda@aiimskalyani.edu.in>, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, <dda@aiimsrbl.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, <dda@aiimsbilaspur.edu.in>, Mukesh Kumar <mac.prasad@gmail.com>, ddaaiimsjammu

<ddaaiimsjammu@gmail.com>, <aps101982@rediffmail.com>, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, Administrative Officer <ao.aiimsmadurai@gmail.com>, <dda@aiimsguwahati.ac.in>, <ddaaiimsawantipora1@gmail.com>, Arvind Thakur <arvind.thakur@nic.in>, : <Ak.biswas57@nic.in>, Suprava Poddar <sup15.81997@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officers of PMSSY-IV Section at - arvind.thakur@nic.in;ak.biswas57@nic.in sup15.81997@gov.in

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

---

2 attachments

Letter (103).pdf
90K

AIIMS Regulations 13112019.pdf
669K

No.: Z-28015/151/2025-PMSSY-IV
Government of India
Ministry of Health and Family Welfare
(PMSSY - IV Section)
***

Room No:745A, Nirman Bhawan, New Delhi
Dated 11-08-2025

To,
The Executive Directors, all new AIIMS

Sub: Framing of Regulation under the AIIMS Act, 1956 as amended by the Act of 2012.

Sirs/Madams,

You are aware that Section 29 of the AIIMS Act mandates every Institute, with the previous approval of the Central Government, to make regulations consistent with the AIIMS Act and the rules made thereunder. Further, proviso to Section 29(2) prescribes that every Institute shall, within three months of the date of the commencement of the AIIMS (Amendment) Act, 2012, make Regulations.

2. In pursuance of the aforesaid Section 29 of the AIIMS Act, AIIMS New Delhi has framed AIIMS Regulations, 2019, which were notified on 21.10.2019 (copy attached). You are requested to clarify whether theAIIMS Regulations, 2019 framed by AIIMS New Delhi have been adopted by the Institute Body of your Institute and share the details with the Ministry on priority for record and reference.

Yours faithfully,

Digitally signed by
ARUN KUMAR BISWAS
Date: 11-08-2025
19:17:19
(Arun Kumar Biswas)
Under Secretary to the Government of India
Tel: 011-23063848

Copy to:
(I) The Dy. Directors (Admin), All new AIIMS

रजिस्ट्री सं० डी० एल०-33004/99 REGD. NO. D. L.-33004/99

भारत का राजपत्र
The Gazette of India

असाधारण
EXTRAORDINARY
भाग III—खण्ड 4
PART III—Section 4
प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 361] नई दिल्ली, सोमवार, अक्तूबर 21, 2019/आश्विन 29, 1941
No. 361] NEW DELHI, MONDAY, OCTOBER 21, 2019/ASVINA 29, 1941

स्वास्थ्य और परिवार कल्याण मंत्रालय

(अखिल भारतीय आयुर्विज्ञान संस्थान)

अधिसूचना

नई दिल्ली, 18 अक्तूबर, 2019

फा.सं. 14-3/69(98)/Coordination Cell/Estt.(Part-II) .—अखिल भारतीय आयुर्विज्ञान संस्थान अधिनियम, 1956 (1956 का 25) की धारा 29 की उपधारा (1) द्वारा प्रदत्त शक्तियों का प्रयोग करते हुए और अखिल भारतीय आयुर्विज्ञान संस्थान विनियम, 1999 को उन बातों के सिवाय अधिक्रांत करते हुए जिन्हें ऐसे अधिक्रमण से पूर्व किया गया है या करने का लोप किया गया है, केंद्रीय सरकार के पूर्व अनुमोदन से निम्नलिखित विनियम बनाता है, अर्थात: -

1.	**संक्षिप्त नाम और प्रारंभ-** (1) इन विनियमों का संक्षिप्त नाम अखिल भारतीय आयुर्विज्ञान संस्थान विनियम, 2019 है। (2) ये राजपत्र में उनके प्रकाशन की तारीख को प्रवृत्त होंगे।
2.	**परिभाषाएं**– (1) इन विनियमों में, जब तक कि संदर्भ से अन्यथा अपेक्षित न हो – (क) 'अधिनियम' से अखिल भारतीय आयुर्विज्ञान संस्थान अधिनियम, 1956 (1956 का 25) अभिप्रेत है; (ख) 'अध्यक्ष' से अधिनियम की धारा 10 की उपधारा (3) के अधीन शासी निकाय के अध्यक्ष से अभिप्रेत है; (ग) "उपनिदेशक" से संस्थान का उपनिदेशक (प्रशासन) अभिप्रेत है; (घ) 'निदेशक' से अधिनियम की धारा 11 की उपधारा (1) के अधीन नियुक्त संस्थान के निदेशक से अभिप्रेत है; (ड.) "मूल नियम" से केंद्रीय सरकार कर्मचारी पर लागू मूल नियम अभिप्रेत है; (च) 'सामान्य वित्तीय नियम' विरचित सामान्य वित्तीय नियम, 2017 और वित्तीय प्रबंधन व नियंत्रण हेतु केंद्रीय सरकार द्वारा समय-समय पर यथा-संशोधित से अभिप्रेत है; (छ) 'अध्यक्ष' से इस अधिनियम की धारा 7 की उपधारा (1) के अधीन केंद्रीय सरकार द्वारा नामित संस्थान का अध्यक्ष

	अभिप्रेत है; (ज) 'नियम' से इस अधिनियम की धारा 28 की उपधारा (1) के अधीन केंद्रीय सरकार द्वारा विरचित नियम अभिप्रेत है; (झ) 'अनुसूची' से इन विनियमनों के लिए उपाबद्ध अनुसूची अभिप्रेत है; (ञ) 'सचिव' से संस्थान और शासी निकाय का सचिव अभिप्रेत है; (ट) 'अनुपूरक नियम' से सरकारी सेवकों पर लागू अनुपूरक नियम अभिप्रेत है; जो मूल नियम के अधीन है (ठ) 'खजाना नियम' से केंद्रीय सरकार का खजाना नियम अभिप्रेत है; (2) उन शब्दों और वाक्यांशों के, जो इन विनियमों में प्रयुक्त है, और परिभाषित नहीं हैं, किंतु अधिनियम में परिभाषित है, वहीं अर्थ होंगे, जो उसमें हैं।
3.	**अध्यक्ष की शक्तियां और कार्य-अध्यक्ष-** की ऐसी शक्तियों का उपयोग और कार्य निष्पादन इस अधिनियम, नियम और अनुसूची 1 सहित इन विनियमों में उल्लिखित है,
4.	**संस्थान की बैठकें-** (1) अध्यक्ष कार्य संचालन के लिए जब भी आवश्यक समझे बैठक कर सकेगा, परंतु एक वर्ष में कम से कम दो बार बैठक अवश्य होगी। (2) (क) संस्थान की बैठक अध्यक्ष द्वारा नियत तारीख और समय पर आयोजित की जाएगी। (ख) बैठक का कार्यवाहियों को अध्यक्ष से अनुमोदन प्राप्त होने के पश्चात निदेशक द्वारा संस्थान के सभी सदस्यों को परिचालित की जाएगी और कार्यवाहियों की पुष्टि के लिए सदस्यों को सात दिन का समय दिया जाएगा। (ग) संस्थान के बैठकों की सभी कार्यवाहियों को सचिव द्वाराइस प्रयोजन हेतु रखी गई कार्यवृत्त पुस्तिका में दर्ज कियाजाएगा और प्रत्येक कार्यवृत्त पर उपस्थित सदस्यों द्वारा सम्यक रूप से पुष्टि किए जाने के पश्चात बैठक का अध्यक्ष हस्ताक्षर करेगा। (3) संस्थान की साधारण बैठक के लिए स्थान, तारीख और समय को विनिर्दिष्ट करते हुए ऐसी बैठक की तारीख से कम से कम दो सप्ताह पूर्व सूचना सचिव द्वारा सदस्यों को या तो इलेक्ट्रॉनिक रूप से या स्पीड पोस्ट द्वारादी जाएगी। सूचना के साथ बैठक की कार्यसूची भी भेजी जाएगी और जहां ऐसा करना संभव न हो, वहां ऐसी कार्यसूची को बैठक से कम से कम दस दिन पूर्व या इलेक्ट्रॉनिक रूप से या स्पीड पोस्ट से भेजा जाएगा। (4) संस्थान की असाधारण बैठक अध्यक्ष द्वारा किसी भी समय संस्थान के अत्यावश्यक कार्य संचालनकेलिए बुलाई जा सकेगी। (5) असाधारण बैठकों के लिए, बैठक के स्थान, तारीख और समय की विनिर्दिष्ट सूचना बैठक की तारीख से कम से कम सात दिन पूर्व सचिव द्वारा अध्यक्ष और सदस्यों को भेजी जाएगी, यदि डाक द्वारा या इलेक्ट्रॉनिक माध्यमों द्वाराया स्पीड पोस्ट द्वारा भेजाजाता है, तो उसे डाक प्रमाणपत्र के अधीनभेजा जायेगा। बैठक से कम से कम तीन दिन पूर्वकार्यसूची को या तो इलेक्ट्रॉनिक माध्यम से या स्पीड पोस्ट से भेजा जाएगा। (6) संस्थान की असाधारण बैठक, संस्थान के नौ से अन्यून सदस्यों के लिखित अनुरोध पर अनुरोध प्राप्ति के सात दिनों के भीतर बुलाई जा सकेगी और अपेक्षितबैठक के सदस्यों द्वारा अनुरोधकरने पर बैठक के प्रयोजन को उपदर्शित किया जाएगा। (7) संस्थान की किसी बैठक में अध्यक्ष की अनुपस्थिति की दशा में,उपस्थित सदस्य ऐसी बैठक की अध्यक्षता करने के लिए अपने में से एक व्यक्ति का चुनाव करेंगे। (8) संस्थान के बैठक की गणपूर्ति सात होगी। (9) अध्यक्ष, बैठक के पूर्व या उसके दौरान किसी समय कार्यसूची में निम्नलिखित को शामिल कर सकता है (i) कामकाज की नई मदें, (ii) कार्यसूची में शामिल अनुपूरक मदें, और ऐसे मदों पर भी विचार किया जाएगा। (10) कोई सदस्य संस्थान की किसी बैठक में कोई संकल्प पेश करने की वांछा रखता है, तो वह सचिव को लिखित में इसकी सूचना देगा जो बैठक की तारीख से पूर्व चौदह दिनों से अन्यून उसके पास पहुंच जाए। जब ऐसी सूचना दी गई हो, तो प्रस्तावित संकल्प सचिव द्वारा सदस्यों को तत्काल परिचालित किया जाएगा और उसे कार्यसूची में शामिल किया जाएगा। (11) सदस्य, अध्यक्ष से पूर्व अनुमोदन प्राप्त करनेके पश्चात वीडियो कांफ्रेंस के माध्यम से भी भाग ले सकता है आगे वीडियो कांफ्रेंस के माध्यम से ऐसी सहभागिता गणपूर्ति के प्रयोजन के लिए गणना में ली जाएगी।

	(12) यदि संस्थान में नामित कोई गैर-सरकारी सदस्य, संस्थान या शासकीय निकाय या स्थायी समितियों की सतत तीन बैठकों में अध्यक्ष की संतुष्टि के किसी वैध कारण के बिना प्रतिभागिता नहीं करता है तो अध्यक्ष के अनुमोदन से, उसकी सदस्यता समाप्त की जा सकेगी। (13) संस्थान द्वारा बैठक के दौरान निपटाए गए किसी विषय को एक वर्ष की समाप्ति पर विचारार्थ नहीं लाया जाएगा सिवाय ऐसे मामले में, जहां अध्यक्ष या सरकार यह प्रमाणित करती है कि संस्थान के हित में विषय पर और विचार करना अपेक्षित है। (14) बैठक में किसी सदस्य द्वारा उठाए गए आदेश के प्रश्न पर अध्यक्ष द्वारा लिया निर्णय अंतिम होगा। (15) संस्थान के सभी निर्णय बहुसंख्यक मत द्वारा लिए जाएंगे और मतों की संख्या समान रहने पर अध्यक्ष का मत निर्णायक होगा। (16) संस्थान का कोई भी कार्य संव्यवहार सदस्यों और अध्यक्ष द्वारा कागजात के परिचालन के माध्यम से किया जाएगा और यदि मतैक्य अनुमोदन होता है तो उस पर कार्रवाई की जाएगी। संकल्प और उस पर की गई कार्रवाई संस्थान की आगामी बैठक में पुष्टि के लिए रखी जाएगी।
5.	**शासी निकाय का गठन -** शासी निकाय में निम्नलिखित ग्यारह सदस्य होंगे, अर्थात:- (क) संस्थान का अध्यक्ष -सभापति ; (ख) स्वास्थ्य सेवा महानिदेशक -पदेन सदस्य; (ग) वित्त मंत्रालय का प्रतिनिधि - पदेन सदस्य; (घ) निदेशक, अखिल भारतीय आयुर्विज्ञान संस्थान -सदस्य ; (ङ) संस्थान में निर्वाचित तीन सदस्यों में से एक को संस्थान के सदस्यों द्वारा निर्वाचित किया जाएगा (च) संस्थान के सदस्यों में से छह सदस्यों को निर्वाचित किया जाएगा (छ) निम्नलिखित स्थायी विशेष आमंत्रित:- (i) अपर सचिव (स्वास्थ्य और परिवार कल्याण मंत्रालय में संस्थान का प्रभारी) ; (ii) संयुक्त सचिव (स्वास्थ्य और परिवार कल्याण मंत्रालय में संस्थान का प्रभारी) ; (iii) डीन (अकादमिक) ; (iv) उपनिदेशक (प्रशासन) ; (v) ज्येष्ठ वित्त सलाहकार
6.	**शासी निकाय की शक्तियाँ और कार्य** — शासी निकाय ऐसी शक्तियों का प्रयोग करेगा और ऐसे कार्यों का निर्वहन करेगा जो अनुसूची I सहित इन विनियमों में अधिकथित हैं।
7.	**अध्यक्ष की शक्तियां और कार्य** — अध्यक्ष ऐसी शक्तियों का प्रयोग करेगा और उन कार्यों का निर्वहन करेगा जो इन विनियमों में अधिकथित है।
8.	**शासी निकाय की बैठकें** — (1) शासी निकास अपने कार्य संचालन हेतु अध्यक्ष द्वारा आवश्यक समझे जाने पर बैठक कर सकती है, लेकिन आमतौर पर जनवरी, मई और सितंबर के महीने में कम से कम तीन बार प्राथमिक रूप से बैठक होंगी। (2) बैठक की कार्रवाई अध्यक्ष के अनुमोदन प्राप्त करने के पश्चात् निदेशक द्वारा शासी निकाय के सदस्यों में प्रचालित की जाएगी। कार्रवाई की पुष्टि के लिए सदस्यों को चौदह दिनों की अवधि दी जाएगी। (3) शासी निकाय की बैठकों की सभी कार्रवाईयों को प्रयोजन के लिए सचिव द्वारा रखी जाने वाली एक कार्यवृत्त पुस्तिका में दर्ज किया जाएगा और उपस्थित सदस्यों द्वारा उपर्युक्त की सम्यक पुष्टि किए जाने के पश्चात् बैठक के अध्यक्ष द्वारा सभी कार्यवृत्त पर हस्ताक्षर किए जाएंगे। (4) शासी निकाय की एक असाधारण बैठक को शासी निकाय के कम से कम छह सदस्यों या अध्यक्ष द्वारा लिखित अनुरोध पर आयोजित की जाएगी। (5) शासी निकाय की प्रत्येक बैठक की सूचना सचिव द्वारा शासी निकाय के सदस्यों को भेजी जाएगी, साधारण बैठक के मामले में कम से कम चौदह दिन और असाधारण बैठक के मामले में कम से कम सात दिन पहले बैठक की तारीख से पहले

	या तो इलेक्ट्रॉनिक रूप से या स्पीड डाक द्वारा भेजे जाने पर डाक प्रमाण पत्र के अधीन बैठकों का कार्यवृत्त भेजा जाएगा यदि डाक या इलेक्ट्रॉनिक रूप से या स्पीड डाक द्वारा तो बैठक की तारीख से क्रमशः कम से कम दस दिन और पांच दिन पूर्व भेजा जाएगा। (6) किसी भी बैठक में अध्यक्ष की अनुपस्थिति में, उपस्थित सदस्य बैठक में अध्यक्षता करने के लिए आपस में एक व्यक्ति का निर्वाचन करेंगे।
	(7) पाँच सदस्यों से गणपूर्ति होगी, अध्यक्ष की पूर्व स्वीकृति प्राप्त करने के पश्चात सदस्य वीडियो कॉन्फ्रेंस के माध्यम से भी बैठक में भाग ले सकते हैं, और वीडियो सम्मेलन के माध्यम से ऐसी भागीदारी को गणपूर्ति के प्रयोज्य हेतु गिनी जाएगी। (8) शासी निकाय के सभी निर्णय बहुमत द्वारा लिए जाएंगे। वोटों की बराबरी की स्थिति में अध्यक्ष का निर्णायक मत होगा। (9) शासी निकाय का कोई भी सदस्य बैठक में किसी भी संकल्प को लाने की वांछा रखता है तो सचिव को उसके बारे में लिखित रूप से नोटिस दिया जाएगा जो कि बैठक की तारीख से कम से कम सात दिन पहले पहुँच जाए। ऐसा नोटिस प्राप्त होने पर सचिव द्वारा सदस्यों को तत्काल प्रचालित किया जाएगा और बैठक के कार्यसूची में शामिल किया जाएगा। (10) कोई भी मामला जो कार्यसूची में शामिल नहीं किया गया हो और जिसकी सूचना उप-विनियम (9) में उल्लिखित के अनुसार नहीं दिया गया हो तो उस पर अध्यक्ष की अनुमति से शासी निकाय की बैठक में विचार किया जा सकता है। (11) शासी निकाय के किसी भी कार्य को सदस्यों और अध्यक्ष को कागजात के संचालन द्वारा हस्तांतरित किया जा सकता है और यदि सर्वसम्मति से सहमति व्यक्त की जाती है तो उस पर कार्रवाई की जाएगी। निर्णय और उस पर की गई कार्रवाई को पुष्टि के लिए शासी निकाय की अगली बैठक में प्रस्तुत किया जाएगा। यदि अगली बैठक में शासी निकाय द्वारा संकल्प की पुष्टि नहीं की जाती है, तो परिचालित व सदस्यों द्वारा सहमत संकल्प के अनुपालन में पूर्व में की गई कार्रवाई ही मान्य होगी। यदि शासी निकाय अगली बैठक में संकल्प की पुष्टि नहीं करता है, तो परिचालित और सदस्यों द्वारा सहमत संकल्प के अनुपालन में पूर्व में की गई कार्रवाई मान्य होगी।
	(12) यदि शासी निकाय में नामांकित एक गैर-सरकारी सदस्य बिना किसी वैध कारण के लगातार तीन बैठकों में अनुपस्थित रहता है, तो अध्यक्ष के अनुमोदन से उसकी सदस्यता समाप्त कर दी जाएगी।
9.	**शासी निकाय के सदस्यों की पदावधि-** (1) यदि शासी निकाय के पदेन सदस्य से भिन्न एक सदस्य की पदावधि संस्थान के एक सतत सदस्य के रूप में पांच वर्ष का होगा और पद छोड़ने वाले सदस्य फिर से निर्वाचन के लिए पात्र होगा। (2) निर्वाचित सदस्यों की आकस्मिक रिक्तियों को संस्थान द्वारा रिक्ति की शेष अवधि के लिए निर्वाचन द्वारा भरा जाएगा।
10.	**शासी निकाय, स्थायी समिति और तदर्थ समिति के अध्यक्ष और सदस्यों के भत्ते —**(1) शासी निकाय, स्थायी समितियों और तदर्थ समितियों के अध्यक्ष और सदस्यों को बैठकों में शामिल होने के लिए यात्रा और दैनिक भत्ते के अलावा कोई वेतन, शुल्क, पारिश्रमिक या अन्य भत्ता नहीं दिया जायेगा। (2) अध्यक्ष और शासी निकाय और स्थायी तथा तदर्थ समितियों के सदस्य, यदि वे केंद्रीय या राज्य सरकार के अधिकारी हैं, तो उन्हें केंद्रीय या राज्य सरकार के अधिकारियों के रूप में आनुज्ञेय दर पर संस्थान द्वारा यात्रा और दैनिक भत्ते का भुगतान किया जाएगा। (3) उप-विनियम (2) में उल्लिखित से भिन्न, शासी निकाय और स्थायी तथा तदर्थ समितियों के अध्यक्ष और सदस्यों के मामलें में यात्रा भत्ते और दैनिक भत्ते का भुगतान उन दरों, जिनके उस संगठन, जहां वे कार्यरत हैं, के नियमों के अनुसार वे हकदार हैं या केन्द्रीय सरकार द्वारा समय पर निर्धारित पूरक नियमों और कार्यकारी निर्णय और उसके अधीन जारी आदेशों के अनुसार जो भी अधिक है, पर किया जायेगा। (4) अध्यक्ष, विशेष कारणों से शासी निकाय, स्थायी और तदर्थ समिति के ऐसे सदस्यों, जो हवाई यात्रा के पात्र नहीं हैं, के लिए हवाई यात्रा की मंजूरी दे सकता है और ऐसी यात्रा के लिए यात्रा भत्ते का भुगतान केंद्रीय सरकार के समूह 'क' अधिकारी के लिए स्वीकार्य दरों पर किया जाएगा।

11.	**निदेशक की शक्तियां और कर्तव्य —** निदेशक अनुपूरक नियमों के नियम 2 के उप-नियम (10) के संदर्भ में संस्थान के प्रमुख होंगे और संस्थान के प्रमुख की शक्तियों का प्रयोग करेंगे और निम्नलिखित कर्तव्यों का निर्वहन करेंगे, अर्थात्: - (क) वह संस्थान के प्रशासन के प्रभारी होंगे। वह संस्थान के अधिकारियों और कर्मचारियों को कार्यों का आवंटन करेंगे और ऐसे पर्यवेक्षण और कार्यकारी नियंत्रण का उपयोग करेगा, जो नियमों और इन विनियमों के अधीन आवश्यक हो सकता है; (ख) वह इन विनियमों के लिए अनुसूची-I में निर्दिष्ट शक्तियों का प्रयोग करेगा; (ग) उसके पास शासी निकाय द्वारा लागू सीमाओं के अधीन प्रशासनिक पक्ष की अपनी कोई भी शक्ति अधिकारियों को प्रत्यायोजित करने का अधिकार होगा।
12.	**स्थायी समितियों के कार्य के संचालन की प्रक्रिया -** (1) सभी स्थायी समितियां सलाहकार समितियां होंगी। (2) सदस्यों का पचास प्रतिशत से सभी स्थायी समितियों के लिए गणपूर्ति होगी। सदस्य अध्यक्ष की पूर्व स्वीकृति प्राप्त करने के पश्चात् वीडियो कॉन्फ्रेंस के माध्यम से भी बैठक में भाग ले सकते हैं, और वीडियो कॉन्फ्रेंस के माध्यम से ऐसी भागीदारी की गणपूर्ति के प्रयोजन के लिए गिना जाएगा। स्थायी चयन समिति या संयुक्त चयन समिति या क्षेत्रीय चयन समिति के मामले में, गणपूर्ति का निर्धारण करने के प्रयोजन के लिए दो विशेषज्ञों को भी गिना जायेगा।
13.	**संस्थान से संबंधित भवन और भूमि —** (1) संस्थान अपने प्रयोजनों के लिए अपनी भूमि और भवनों का उपयोग करेगा। (2) आवंटन और मूल्यांकन तथा इमारतों के किराए की वसूली निदेशक द्वारा मूल नियम के नियम 45क, नियम 45ख और नियम 45ग और पूरक नियमों के उपबंधों के अनुसार की जायेगी। (3) संस्थान के हर कर्मचारी को , अगर संस्थान के परिसर में आवास का प्रस्ताव किया जाता है तो वे उस आवास में रहेंगे और संस्थान द्वारा निर्धारित किराये और अन्य प्रभारों का भुगतान करेंगे।
14.	**पुरस्कार, छात्रवृत्ति देने की शक्तियाँ** - संस्थान समय-समय पर अपने छात्रों को शासी निकाय द्वारा निर्धारित पुरस्कार, स्मृति चिन्ह, वृत्तिका और छात्रवृत्ति प्रदान कर सकता है।
15.	**संकायाध्यक्ष और सह-संकायाध्यक्ष की नियुक्ति की प्रक्रिया** - (1) तीन संकायाध्यक्ष होंगे, अर्थात् संकायाध्यक्ष (शैक्षिक), संकायाध्यक्ष (अनुसंधान) और संकायाध्यक्ष (परीक्षा)। आचार्य और विभागाध्यक्ष को निदेशक के परामर्श से ज्येष्ठता को ध्यान में रखते हुए संस्थान द्वारा संकायाध्यक्ष के रूप में नियुक्त किया जाएगा। (2) तीन सह-संकायाध्यक्ष होंगे, अर्थात सह-संकायाध्यक्ष (शैक्षिक), सह-संकायाध्यक्ष (अनुसंधान), और सह-संकायाध्यक्ष (परीक्षा)। किसी भी शिक्षक वर्ग (अपर आचार्य या उससे ऊपर) को निदेशक के परामर्श से संस्थान द्वारा सह-संकायाध्यक्ष के रूप में नियुक्त किया जा सकता है। सह- संकायाध्यक्ष (शैक्षिक) और सह-संकायाध्यक्ष (अनुसंधान) को मेडिकल संकाय से ही नियुक्त किया जाएगा। (3) संकायाध्यक्ष और सह-संकायाध्यक्ष का कार्यकाल अधिकतम तीन वर्ष का होगा और संस्थान के निदेशक के परामर्श से संस्थान द्वारा एक और कार्यकाल के लिए और आगे बढ़ाया जा सकेगा। (4) संकायाध्यक्ष और सह-संकायाध्यक्ष विद्यमान संकाय सदस्यों से नियुक्त किए जाएंगे और जब तक कि भारत सरकार द्वारा समय-समय पर अनुमोदित नहीं किया जाता है, तब तक कोई अतिरिक्त पारिश्रमिक का भुगतान नहीं किया जाएगा।
16.	**आचार्य पद .** - संस्थान आचार्य पद, अपर आचार्य पद, उप-आचार्य पद, सहायक आचार्य पद, प्राध्यापक पद, नर्सिंग कॉलेज के आचार्य सह-प्राचार्य, नर्सिंग कॉलेज के आचार्य- सह-उप-प्राचार्य, नर्सिंग में सह-आचार्य, नर्सिंग में सहायक आचार्य और अन्य पद सृजित कर सकता है और व्यक्तियों को नियुक्त कर सकता। भारत सरकार की स्वीकृति के बिना कोई पद सृजित नहीं किया जाएगा।

17.	**व्याख्यान की व्यवस्था करने की शक्ति -** यह संस्थान समुचित शुल्क या मानदेय के भुगतान पर समय-समय पर संस्थान में व्याख्यान देने के लिए विशेषज्ञों को आमंत्रित कर सकता है और उन्हें भारत के भीतर अपनी यात्रा के लिए के केंद्रीय सरकार के समान स्थिति कर्मचारियों के लिए स्वीकार्य दरों पर यात्रा भत्ते का भुगतान कर सकता है।
18.	**शुल्क और अन्य प्रभार -** संस्थान के विभिन्न पाठ्यक्रमों में प्रवेश के लिए चयनित उम्मीदवारों द्वारा देश सभी शुल्क और अन्य प्रभार अकादमिक समिति द्वारा संस्तुत और स्थायी वित्त समिति, शासी निकाय और संस्थान द्वारा समय-समय पर अनुमोदित दरों के अनुसार होंगे।
19.	**अध्ययन के पाठ्यक्रमों में प्रवेश -** अनुसूचित जाति (एससी), अनुसूचित जनजाति (एसटी), अन्य पिछड़ा वर्ग (ओबीसी), आर्थिक रूप से कमजोर वर्ग (ईडब्ल्यूएस) और अन्य श्रेणियों के लिए आरक्षण भारत सरकार द्वारा समय-समय पर निर्धारित नीति के अनुसार होगा।
20.	**उपाधियाँ प्रदान करना -** संस्थान एमबीबीएस, एमडी, एमएस, पीएच-डी, डीएम, एमसीएच,एमएचए, एमडीएच, फैलोशिप, एमएससी, एम.बायोटेक, बी.एससी (ऑनर्स) ह्यूमन बायोलॉजी, बी.एससी (ऑनर्स) नर्सिंग, बी.एससी। नर्सिंग (पोस्ट-सर्टिफिकेट), बी.एससी(ऑनर्स) पैरामेडिकल विषयों और किसी भी अन्य डिग्री के रूप में संस्थान की स्थायी शैक्षणिक समिति द्वारा अनुमोदित और शासी निकाय द्वारा किए गए अनुसमर्थन से, संस्थान जिसे वांछनीय समझता है, वह डिग्री मंजूर कर सकता है।।
21.	**परीक्षा का आयोजन (शैक्षणिक के साथ- साथ में भर्ती) -** संस्थान में परीक्षा आयोजित करने, प्रश्न-पत्र तैयार करने, उत्तर पुस्तिकाओं या शोध पत्रों, मौखिक और प्रैक्टिकल परीक्षा की जांच करने, के लिए निदेशक द्वारा अपेक्षित संख्या में पर्यवेक्षकों, निरीक्षकों, परीक्षकों (आंतरिक बाहरी) और अन्य कर्मचारियों की नियुक्ति की जा सकती है और शैक्षणिक समिति द्वारा की गई संस्तुति तथा स्थायी वित्त समिति, शासी निकाय और संस्थान द्वारा समय-समय पर किए गए अनुमोदन के अनुसार उन्हें पारिश्रमिक का भुगतान किया जा सकता है।
22.	**पूर्णकालिक कर्मचारी -** जब तक, किसी भी मामले में, अन्यथा यह स्पष्ट रूप से प्रदान नहीं किया जाता संस्थान के कर्मचारी का पूरा समय संस्थान के अधीन होगा और उसे बिना किसी अतिरिक्त पारिश्रमिक का दावा किए बगैर संस्थान के समुचित प्राधिकारी द्वारा अपेक्षित तरीके से नियोजित किया जा सकता है।
23.	**स्थायी और अस्थायी पद —** (1) संस्थान की सेवा में पद किसी भी समय-सीमा के बिना स्वीकृत वेतन की एक निश्चित दर पर स्थायी पद होंगे या सीमित समय के लिए स्वीकृत पद की निश्चित दर पर अस्थायी पद होंगे। स्थायी पद धारित किसी व्यक्ति की एक निर्धारित अवधि के लिए उच्च पद पर नियुक्ति होने पर उसे प्रारंभ में अधिकतम पांच वर्ष की अवधि के लिए पूर्वधारित पद में अपना धारणाधिकार रखने की अनुमति होगी जिसे दो वर्ष या समयपूर्व प्रत्यावर्तन के लिए बढ़ाया जा सकेगा। (2) निवासी डॉक्टरों के अस्थायी पदों को भारत सरकार के स्वास्थ्य और परिवार कल्याण मंत्रालय की समय-समय पर संशोधित की गई रेजिडेंसी योजना द्वारा नियंत्रित किया जाएगा।
24.	**नियुक्ति के लिए योग्यता —** (1) उम्मीदवारों से आवेदन आमंत्रित करने से पहले समान पदों के लिए केंद्रीय सरकार द्वारा निर्धारित योग्यता और अनुभव को ध्यान में रखते हुए संस्थान के तहत किसी पद पर नियुक्ति के लिए आयु, अनुभव और अन्य योग्यताएं नियुक्ति प्राधिकारी द्वारा निर्धारित की जाएंगी, परन्तु गैर-चिकित्सा कर्मियों की नियुक्ति निदेशक के पद पर नहीं की जाएगी जिसे नियुक्ति प्राधिकारी के अनुमोदन के पश्चात समय-समय पर अलग से अधिसूचित किया जाएगा। (2) निदेशक, संस्थान के तहत पदों और सेवाओं में रिक्त पदों को भरने के लिए, अनुसूचित जातियों, अनुसूचित जनजातियों, अन्य पिछड़े वर्गों, आर्थिक रूप से कमजोर वर्गों और अन्य श्रेणियों के पक्ष में इस तरह के आरक्षण करेगा, जो केंद्रीय सरकार के अधीन पदों और सेवाओं में रिक्त पदों को भरने के लिए समय-समय पर किए जाते हैं।
25.	**परिवीक्षा की अवधि -** यदि किसी भी मामले में नियुक्ति प्राधिकारी द्वारा अन्यथा तय नहीं किया गया है, सभी कर्मचारी दो साल के लिए परिवीक्षा पर रहेंगे। परिवीक्षा की अवधि के दौरान, कर्मचारी को संतोषजनक सेवा देनी होगी ऐसा न करने पर किसी भी समय या कोई भी नोटिस या कारण बताए बगैर उसकी सेवाएं समाप्त कर दी जाएगी। हालांकि, नियुक्ति प्राधिकारी परिवीक्षा की अवधि बढ़ा सकता है।
26.	**ज्येष्ठता -** संस्थान के प्रत्येक श्रेणी के कर्मचारियों की ज्येष्ठता का निर्धारण उसकी योग्यता के क्रम से किया जाएगा जिसमें उन्हें संबंधित पद पर नियुक्ति के लिए चुना गया था, जिन्हें पहले चुना गया था, उन्हें बाद में चयनित कर्मचारियों से ज्येष्ठ दर्जा दिया जाएगा।

27.	**छुट्टी** - (1) संस्थान के अस्थायी और स्थायी कर्मचारी इस तरह के अवकाश और अवकाश वेतन के हकदार होंगे जो केंद्रीय सिविल सेवा (अवकाश) नियम, 1972 के तहत केंद्रीय सरकार के कर्मचारियों की समान श्रेणियों के लिए अनुमन्य हैं। परंतु केंद्रीय सरकार के केंद्रीय सिविल सेवा (छुट्टी) नियम, 1972 के प्रयोजन हेतु, संस्थान में अध्यापन कर्मचारीवृंद की निम्नलिखित श्रेणियों या किसी अन्य पद को स्थायी शैक्षणिक समिति द्वारा अकादमिक पद के रूप में घोषित किया गया हो और शासी निकाय द्वारा समय-समय पर इसकी पुष्टि की गई हो, को छुट्टी विभाग में सेवारत कर्मचारी के रूप में माना जाएगा, अर्थात्: - (1) आचार्य, (2) अपर आचार्य, (3) सह आचार्य, (4) सहायक आचार्य, (5) चिकित्सा अधीक्षक, (6) अपर चिकित्सा अधीक्षक, (7) प्राचार्य, नर्सिंग महाविद्यालय, (8) नर्सिंग प्राध्यापक, (9) ज्येष्ठ नर्सिंग शिक्षक, और (10) नर्सिंग शिक्षक: (2) इस प्रयोजन के लिए नियमित अवकाश समय-समय पर शासी निकाय द्वारा किए गए निर्णय के अनुसार होगा। परन्तु संस्थान में प्रतिनियुक्ति पर एक पदधारी को अन्यत्र सेवा के रूप में छुट्टी के उन नियमों द्वारा शासित किया जाएगा, जिन्हें उनके प्रतिनियुक्ति की शर्तों में निर्धारित किया गया है।
28.	**पेंशन और अंशदायी भविष्य निधि** - (1) 12 सितंबर, 1975 को या उसके बाद नियुक्त किए गए संस्थान के कर्मचारी, संस्थान में अन्यत्र सेवा में प्रतिनियुक्त कर्मचारियों को छोड़कर, और ऐसे कर्मचारी जिन्हें इस तिथि से पहले नियुक्त किया गया था, लेकिन उन्होंने विशेष रूप से केंद्रीय सरकार के कर्मचारियों के लिए लागू सामान्य भविष्य निधि और पेंशन लाभों को ऐसे कर्मचारी से चुना है, सामान्य भविष्य निधि (केंद्रीय सेवा) नियम, 1960 और केंद्रीय सिविल सेवा (पेंशन) नियम, 1972 के प्रावधानों द्वारा शासित होंगे। (2) 1 जनवरी, 2004 से, जब से नई पेंशन योजना शुरू हुई थी, 1 जनवरी 2004 को या उसके बाद संस्थान की सेवा में शामिल होने वाले सभी नए कर्मचारियों को नई पेंशन योजना द्वारा शासित किया जाएगा।
29.	**कार्य से अनुपस्थिति** – जब तकअसाधारण परिस्थितियों में राष्ट्रपति द्वारा अन्यथा एवं कोई निर्णय नहीं लिया जाता, संस्थान का कोई भी स्थायी कर्मचारी अवकाश पर रहने या लिम्बन के कारण शासी निकाय द्वारा इस संबंध में समय-समय पर अनुमोदित दिशा-निर्देशों में उल्लिखित अवधि और प्रयोजनों के अतिरिक्त अनुपस्थित नहीं रहेगा।
30.	**अधिवर्षिता** - (1) संस्थान के अध्यापन संकाय के अलावा कर्मचारी की सेवानिवृत्ति की आयु साठ वर्ष या भारत सरकार द्वारा समय-समय पर विनिर्दिष्ट आयु के अनुसार होगी: परन्तु उन व्यक्तियों के मामले में, जो कारणों को अभिलिखित करने के लिए विशेष रूप से सक्षम हैं तथा शारीरिक रूप से स्वस्थ तथा संबंधित व्यक्ति की निरंतर दक्षताके अधीन वैज्ञानिक विशेषज्ञों को मामला दर मामला के आधार पर सेवा में बासठ वर्ष की आयु तक सेवा विस्तार दिया जा सकता है। (2) संस्थान के शिक्षण संकाय के सदस्य की सेवानिवृत्ति की आयु यथा विनिर्दिष्ट आयु भारत सरकार द्वारा समय-समय पर होगी। **(3)** उप-विनियम (1) और उप-विनियम (2) में किसी बात के होते हुए, नियुक्ति प्राधिकारी के विचार कर सकेगा कि ऐसा करना लोकहित में है, संस्थान के किसी कर्मचारी को कम से कम तीन महीने का लिखित में सूचना देकर या ऐसे सूचना के स्थान पर तीन महीने का वेतन और भत्तों का भुगतान कर नियुक्ति प्राधिकारी उसे सेवानिवृत्त कर सकता है-

	(i) यदि वह समूह क या समूह ख सेवा या पद पर है और उसने पैतीस वर्ष की आयु पूरा करने से पहले संस्थान के सेवा में प्रवेश किया था। तत्पश्चात् उसने पचास वर्ष की आयु प्राप्त कर ली है; और (ii) किसी अन्य मामले में, उसके पचास वर्ष की आयु प्राप्त करने के पश्चात् : परन्तु इस उप - विनियमन में कुछ भी समूह घ सेवा या ऐसे पद के किसी कर्मचारी पर लागू नहीं होगा जो दिनांक 1 दिसंबर, 1962 को या उससे पहले सेवा में प्रवेश किया है। (4) संस्थान का कोई भी कर्मचारी, नियुक्ति प्राधिकारी को लिखित रूप में तीन महीने से अन्यून समय का सूचना देकर, सेवा से सेवानिवृत्त हो सकता है, यदि वह समूह क या समूह ख सेवा या पद पर है, और उसने पैतीस वर्ष की आयु प्राप्त करने से पहले संस्थान की सेवा में प्रवेश किया हो और अन्य सभी मामलों में उसके पचास वर्ष की आयु प्राप्त करने के पश्चातः परन्तु - (क) इस उप - विनियमन में कुछ भी समूह घ सेवा या पद के किसी कर्मचारी पर लागू नहीं होगा जो दिनांक 1 दिसंबर, 1962 को या उससे पहले सेवा में प्रवेश किया है। (ख) यह निलंबन के अधीन कर्मचारी को अनुमति रोकने के लिए नियुक्ति प्राधिकारी के लिए खुला होगा जो इस उप - विनियमन के तहत सेवानिवृत्त होना चाहता है । ***स्पष्टीकरण***.- इस विनियमन में " शिक्षण संकाय के सदस्य " शब्दों का तात्पर्य आचार्य, अपर आचार्य, सह-आचार्य, सहायक आचार्य, चिकित्सा अधीक्षक, अपर चिकित्सा अधीक्षक, नर्सिंग कॉलेज का प्राचार्य, नर्सिंग में प्राध्यापक, ज्येष्ठ नर्सिंग शिक्षक और नर्सिंग में शिक्षक और समय-समय पर केंद्रीय सरकार द्वारा शिक्षण संकाय के सदस्यों के रूप में घोषित किए जाने वाले संस्थान के अन्य कर्मचारियों से है।
31.	**निदेशक के पद का कार्यकाल । -** (1) निदेशक का कार्यकाल पद धारण से पाँच वर्षों या 65 वर्ष की आयु प्राप्त करने, इसमें से जो भी पहले हो, तक होगा। (2) इन विनियमनों में किसी बात के होते हुए भी, यदि का मत है कि यदि ऐसा करना जनहित में है तो उसे लिखित रूप में तीन महीने से अन्यून की सूचना देकर या इसके एवज में तीन महीने के वेतन और भत्ते देकर उसके कार्यकाल की समाप्ति से पहले किसी भी समय निदेशक के पद के कार्यकाल को समाप्त करने का अधिकार होगा । निदेशक को यह भी अधिकार होगा कि वह संस्थान को लिखित रूप में तीन महीने से अन्यून समय का नोटिस देकर निश्चित कार्यकाल समाप्त होने से पहले किसी भी समय अपने पद को त्याग सकता है ।
32.	**भर्ती आयु** — संस्थान की सेवा में भर्ती के समय उम्मीदवार की अधिकतम आयु शिक्षण पदों के लिए सामान्य रूप से पचास वर्ष और गैर शिक्षण पदों के लिए तीस वर्ष होगी या जैसा कि प्रत्येक पद के लिए भर्ती नियमों में दर्शाया गया है (अखिल भारतीय आयुर्विज्ञान संस्थान के सभी विभागों में ज्येष्ठ प्रदर्शकों या ज्येष्ठ रेजिडेंटों को छोड़कर जहां यह तीस वर्ष होगी या जैसी समय-समय पर स्थायी अकादमिक समिति द्वारा सिफारिश की जाती है)। शासी निकाय द्वारा इस सीमा में छूट दी जा सकती है।
33.	**आचरण, अनुशासन और दंड —— (1**) केंद्रीय सिविल सेवा (आचरण) नियम, 1964 जिसमें समय-समय पर यथा-उपांतरित होता है, संस्थान के कर्मचारियों पर लागू होगा । (2) केन्द्रीय सिविल सेवा (वर्गीकरण, नियंत्रण और अपील) नियम , 1965 का भाग IV (निलंबन) , भाग V (दंड और अनुशासनात्मक प्राधिकारी) भाग VI (दंड अधिरोपित करने संबंधी प्रक्रिया) , भाग VII (अपील) और भाग VIII (समीक्षा) जिसमें समय-समय पर यथा-उपांतरित होता है, संस्थान के कर्मचारियों पर लागू होगा :

	परंतु इस विनियमन के प्रयोजन के लिए , - (क) संस्थान में समूह क, समूह ख, समूह क और समूह घ पद क्रमशः केंद्रीय सिविल सेवा समूह क, समूह ख, समूह ग और समूह घ पद के अनुरूप होंगे; (ख) संस्थान के विभिन्न पदों के लिए नियुक्ति प्राधिकारी, दंडों के लिए अनुशासनात्मक प्राधिकारी जिन्हें अध्यारोपित किया जा सकता है और अपीलीय प्राधिकारी अनुसूची-II के अनुरूप होंगे। (ग) संस्थान द्वारा उधार लिए गए केंद्रीय या राज्य सरकार के सेवकों के संबंध में, केंद्रीय सिविल सेवा (वर्गीकरण, नियंत्रण और अपील) नियम, 1965 के क्रमशः नियम 20 और नियम 21 के प्रावधान लागू होंगे और संस्थान इन नियमों के प्रयोजन के लिए जैसा भी मामला हो केंद्रीय या राज्य सरकार के कार्यों का उपयोग करेंगे; (घ) किसी भी मामले में संघ लोक सेवा आयोग से कोई परामर्श आवश्यक नहीं होगा ।
34.	**कर्मचारियों के लिए चिकित्सा सुविधाएं —** (1) संस्थान के कर्मचारी जिनमें प्रतिनियुक्तिकर्ता और उनके परिवार के सदस्य शामिल हैं , अखिल भारतीय आयुर्विज्ञान संस्थान की कर्मचारी स्वास्थ्य योजना के तहत स्वीकार्य चिकित्सा सहायता के हकदार होंगे । वे भी इस तरह के अंशदान का भुगतान करेंगे जैसा कि उस योजना के तहत अपेक्षित है । (2) संस्थान के सेवानिवृत्त कर्मचारियों और उनके परिवारों के सदस्यों के साथ-साथ उन कर्मचारियों और उनके परिवार के सदस्यों के मामले में जो संस्थान के स्थान के अलावा अन्य स्थानों पर चिकित्सा सुविधाओं का लाभ उठाते हैं, केंद्रीय सेवा चिकित्सा परिचारक नियम, 1944 जिसमें समय-समय पर संशोधन होता है, लागू होगा। किसी भी परेशानी में, इस तरह के मामलों में खर्च चिकित्सा व्यय की प्रतिपूर्ति केन्द्र सरकार स्वास्थ्य योजना की लागू दरों के अनुसार की जाएगी।
35.	**सेवा की अन्य शर्तें –** इन विनियमनों में नहीं दिए गए मामलों के संबंध में, सेवा की सामान्य शर्तों, वेतन, यात्रा और दैनिक भत्ते, अवकाश वेतन, कार्यग्रहण अवधि, विदेश सेवा संबंधी शर्तों और समय-समय पर केन्द्र सरकार द्वारा जारी आदेशों एवं निर्णयों के संबंध में केन्द्रीय सरकार के कर्मचारियों पर लागू नियम संस्थान के कर्मचारियों पर लागू होंगे।
36.	**कर्मचारियों को संस्थान निवास का आवंटन -** संस्थान के कर्मचारियों प्रावधानों समय-समय पर संस्थान द्वारा अधिकथित मेडिकल साइंसेज अखिल भारतीय आयुर्विज्ञान संस्थान में आवासों के आवंटन के लिए हकदार होगा ।

अनुसूची-I

(विनियमन 3, 6 और 11 देखें)

शक्तियों का विस्तार

क्र.सं.	शक्तियों की प्रकृति	निदेशक	अध्यक्ष	शासी निकाय	संस्थान	टिप्पणियां
(1)	(2)	(3)	(4)	(5)	(6)	(7)
1.	स्वीकृत बजट से निधियों के पुन:विनियोजन की शक्तियां	पूर्ण शक्तियां	-	-	-	किसी भी पुन: विनियोजन की रिपोर्ट को उसके बाद की बैठक में अनुमोदन के लिए शासी निकाय के समक्ष रखा जाएगा।
2.	(i) धोखाधड़ी के कारण जनता के धन के भंडार के	प्रत्येक मामले में रु.। 2,000/- तक	प्रत्येक मामले में रु.। 0,000/- तक	प्रत्येक मामले में रु. 20,000/-	पूर्ण शक्तियाँ	

	अपरिवर्तनीय मूल्य के नुकसान को बट्टे खाते डालना।			तक		
	(ख) राजस्व या अपरिवर्तनीय अग्रिम का नुकसान					
	(ग) भंडार के मूल्य में कमी और मूल्यह्रास					
3.	स्टोर्स और स्टेशनरी की खरीद और प्रपत्रों की छपाई पर (i) आकस्मिक व्यय (या) व्यय करना।	स्वीकृत बजट के भीतर पूर्ण शक्तियां।	-	-	-	-
4.	भवन का रखरखाव और खुदरा कार्य: -	-		-	-	-
	(क) मूल कार्य और विशेष मरम्मत	अधिकतम रु. एक लाख प्रति वर्ष के अधीन प्रत्येक मामले में रु. 20,00,000/-	अधिकतम रु. 25 लाख प्रति वर्ष के आधार पर प्रत्येक मामले में रु. 50,000/-	-	-	-
	(ख) साधारण मरम्मत	मामूली मरम्मत के लिए पूर्ण अधिकार (वार्षिक मरम्मत नहीं)	-	-	-	-
	(ग) वार्षिक मरम्मत	पूर्ण शक्तियाँ	-	-	-	-
5.	वसूली योग्य अग्रिमों को मंजूरी देने की शक्ति	स्वयं को छोड़कर सभी अधिकारियों और कर्मचारियों के संबंध में पूर्ण अधिकार	निदेशक के मामले में	-	-	-
6.	अंशदायी/ सामान्य भविष्य निधि में से अग्रिम / अंतिम निकासी की मंजूरी की शक्ति	स्वयं को छोड़कर सभी अधिकारियों और कर्मचारियों के संबंध में पूर्ण अधिकार	निदेशक के मामले में	-	-	-
7.	खातों के साथ जुड़े आधिकारिक रिकॉर्ड को समाप्त करना	सामान्य वित्तीय नियमों के के परिशिष्ट 13 में निर्धारित शर्तों के अधीन पूर्ण शक्तियां	-	-	-	-
8.	किसी महीने के अंतिम कार्य दिवस पर भुगतान निर्देशित करने की शक्ति, जो संस्थान के कर्मचारियों के वेतन और भत्ते, जहां अगले महीने के पहले चार दिन सार्वजनिक अवकाश हो।	पूर्ण शक्तियाँ	-	-	-	-

9.	किसी भी अवधि के लिए निर्विवाद वेतन और स्थापना के भत्ते को तीन महीने से अधिक नहीं रखने का आदेश देने की शक्ति	पूर्ण शक्तियाँ	-	-	-	-
10.	सबसे छोटा या सस्ता के अलावा अन्य मार्ग से लाभ भत्ते की अनुमति देना	मार्ग का चयन संस्थान के हित में होने पर पूर्ण शक्तियां	-	-	-	-
11.	समूह 'घ' के कर्मचारियों को ट्रेन में एक अधिकारी के साथ अगले उच्च श्रेणी रेलवे किराया लेने की अनुमति देना, जिसमें द्वितीय श्रेणी का प्रावधान किया गया है	पूर्ण शक्तियाँ				
12.	यह तय करना कि देश के भीतर ड्यूटी पर कोई विशेष अनुपस्थिति है या नहीं	शैक्षिक उद्देश्य के लिए पूर्ण शक्तियां और अन्य मामलों में एक माह	शैक्षणिक के अलावा सभी मामलों में एक माह से अधिक पूर्ण शक्तियां	-	-	-
13.	समूह 'ग' और समूह 'घ' के कर्मचारियों द्वारा सार्वजनिक या किराए के वाहन में यात्रा करने के लिए दैनिक भत्ते के माइलेज भत्ते के आदान-प्रदान पर प्रतिबंध लगाना।	पूर्ण शक्तियाँ				
14.	अपने स्वयं और अन्य कर्मचारियों के यात्रा भत्ता बिलों को प्रतिहस्ताक्षरित करना।	पूर्ण शक्तियाँ	-	-	-	-
15.	अनुपूरक नियम 209 के प्रावधानों को माफ करना और अवकाश के साथ छुट्टियों के संयोजन के बारे में अनुपूरक नियम 211 से प्रस्थान को अधिकृत करना।	पूर्ण शक्तियाँ	-	-	-	-
16.	(i) आकस्मिक अवकाश की मंजूरी	पूर्ण शक्तियाँ	निर्देशक की आकस्मिक छुट्टी।	-	-	-
	(ii) अवकाश की मंजूरी	समूह ख, ग, घ के लिए पूर्ण शक्तियाँ और क के लिए चार सप्ताह से अधिक नहीं।	समूह 'क' के लिए चार सप्ताह से अधिक के लिए पूर्ण शक्तियां और निदेशक के मामले में पूर्ण शक्तियाँ	-	-	-
	(iii) विशेष विकलांगता अवकाश			पूर्ण शक्तियाँ	-	-

17.	यह निर्देश देना कि छुट्टी पर जाने वाला अधिकारी को आवास के पोजेशन में माना जाएगा	मूल प्रतिनियुक्ति की अवधि या स्वीकृत अवकाश की अवधि के लिए पूर्ण शक्तियां	-	पूर्ण शक्तियाँ	-	-
18.	आवास आवंटित करना	पूर्ण शक्तियाँ	-	-	-	-
19.	अखिल भारतीय आयुर्विज्ञान संस्थान नियम 1958 के नियम 7 के अधीन पदों पर नियुक्तियाँ करने की शक्ति।	पूर्ण शक्तियाँ	-	-	-	-
19	(i) तदर्थ/अस्थायी	समूह ख, ग और घ के लिए पूर्ण शक्तियां और व्याख्याता, सहायक प्रोफेसर और एसोसिएट प्रोफेसर के लिए एक वर्ष की अवधि से अधिक नहीं।	संकाय पदों के अलावा सभी समूह 'क' पदों के लिए पूर्ण शक्ति। प्रोफेसर और अतिरिक्त प्रोफेसर के लिए एक साल से अधिक की अवधि के लिए नहीं और व्याख्याता, सहायक प्रोफेसर और एसोसिएट प्रोफेसर के लिए एक साल से अधिक की अवधि के लिए।	-	-	-
	(ii) स्थायी	समूह ग और घ पद	समूह ख पद	समूह क पद	-	-
20.	परिवीक्षा की अवधि के सफल समापन के बाद, समूह क और ख अधिकारियों की पुष्टि करने की शक्ति।	निदेशक के मामले में पूर्ण अधिकार	-	-	-	-
21.	समूह घ कर्मचारियों के इस्तीफे को स्वीकार करने की शक्ति	पूर्ण शक्तियां	-	-	-	-
22.	समूह "क" कर्मचारियों के इस्तीफे को स्वीकार करने की शक्तियां	प्रोफेसर और अतिरिक्त प्रोफेसर के मामले को छोड़कर सभी समूह "क" अधिकारियों के संबंध में पूर्ण शक्तियां	निदेशक, प्रोफेसर और अतिरिक्त प्रोफेसर के मामले में पूर्ण शक्तियां	-		निदेशक के मामले में संस्थान द्वारा अनुसमर्थन के अधीन
23.	बैठक, सम्मेलन, संगोष्ठी, कार्यशाला, संगोष्ठी में भाग लेने या लघु कार्य के लिए विदेश जाने के दौरान संस्थान के अधिकारियों को अनुमति देने की शक्ति	तीस दिनों की अवधि तक देय और अनुज्ञेय अवकाश के आधार पर निदेशक के मामले को छोड़कर पूर्ण शक्तियां, और संबंधित संकाय सदस्यों को बैठक के प्रायोजकों से उचित निमंत्रण मिलता है	कर्मचारियों के मामले में 30 दिनों की अवधि से अधिक के लिए पूर्ण शक्तियां और निदेशक के संबंध में पूर्ण शक्तियां	-		समय-समय पर केंद्र सरकार द्वारा जारी निर्देशों के अधीन

24.	फैक्लटी के सदस्यों द्वारा अंतर्राष्ट्रीय वैज्ञानिक सम्मेलनों/संगोष्टियों/सेमिनारों/विदेश में सहभागिता में कार्य के रूप में अनुपस्थिति के निपटान हेतु शक्ति।	यात्रा सहित अधिकतम 15 दिनों तक पूर्ण शक्तियां	15 दिन की अवधि से परे पूर्ण शक्तियां	-		समय-समय पर केंद्र सरकार द्वारा जारी किए गए निदेशों के शर्ताधीन
25.	ऐसे कर्मचारियों के लिए संस्थान में लियन को बनाए रखने की मंजूरी, जब वे कहीं और तैनात हैं।	समूह 'ग' और 'घ' पदों के लिए अधिकतम दो वर्षों, एक बार में एक वर्ष, तक पूर्ण शक्तियां	समूह "ख" पदों के लिए पूर्ण शक्तियां	समूह "क" पदों के लिए पूर्ण शक्तियां	-	-
26.	संस्थान के कर्मचारियों के वेतन का संबंधित नियमावली के अंतर्गत निर्धारण हेतु शक्ति	पूर्ण शक्तियां	-	-	-	-
27.	संस्थान के अधिकारियों को संस्थान के कार्यों के संबंध में विदेश जाने के लिए संबंधित अधिकारियों को मंजूरी देने की शक्ति और ड्यूटी के रूप में उनकी अनुपस्थिति का निपटान करने की शक्ति	30 दिनों तक उपलब्ध करायी गयी पूर्ण शक्तियों का कोई वित्तीय निहितार्थ नहीं है अपितु संस्थान के कार्य के संबंध में व्यतीत समयावधि को कार्य के रूप में देखा जा रहा है।	30 दिन की अवधि से परे पूर्ण शक्तियां			समय-समय पर केंद्र सरकार द्वारा जारी किए गए निदेशों के शर्ताधीन
28.	यदि अनुसंधान अनुदान तीन वर्ष की अवधि से अधिक के लिए नहीं है तो इन्हें स्वीकृत करने की शक्ति	भारत सरकार की सामान्य नीति के अधीन पूर्ण शक्तियां	-	-	-	
29.	ऐसे मामालों में जहां शर्तें और अनुदेश सामान्य प्रकृति के हैं, केंद्रीय/राज्य सरकार के प्रतिनियुक्त अधिकारी के संबंध में विदेशी सेवा शर्तों पर शर्तें एवं अनुदेश स्वीकृत करने की शक्ति	पूर्ण शक्तियां	-	-	-	-
30.	वरिष्ठ रेजिडेंटों/ट्यूटरों की कालावधि के विस्तार प्रदान करने की शक्ति	पूर्ण शक्तियां	-	-	-	-
31.	चयन समिति की सिफारिशों पर अग्रिम वृद्धि प्रदान करने की शक्ति	तीन अग्रिम वृद्धियों तक पूर्ण शक्ति	तीन अग्रिम वृद्धियों से परे पूर्ण शक्ति	-	-	-

32.	अनुसंधान स्कीमों के कर्मचारियों को संस्थान में नियमित पदों पर उनकी नियुक्ति किए जाने पर मूल नियमावली 27 के तहत अग्रीम वृद्धि प्रदान करने की शक्ति	प्रत्येक मामले की योग्यता के आधार पर पूर्ण शक्तियां	-	-	-	-
33.	ऐसे मामलों में जहां जीवन निर्वाह भत्ता दैनिक भत्ते की प्रकृति में प्राप्त किया जाता है और इसमें मानदेय भी सम्मिलित होता है, में अनुपूरक नियमावली 12 के प्रावधानों में छूट देने की शक्ति	पूर्ण शक्तियां	-	-	समय-समय पर केंद्र सरकार द्वारा जारी किए गए निदेशों के शर्ताधीन	-
34.	किसी संस्थागत कर्मचारी को एक मंत्रालीय कर्मचारी घोषित करना।	पूर्ण शक्तियां	-	-	-	-
35.	किसी लियन को समाप्त करना।	पूर्ण शक्तियां व शर्तें वह व्यक्ति लियन पर धारित पद पर नियुक्ति लेने के लिए प्राधिकृत है।	सभी अन्य पदों के लिए पूर्ण शक्तियां	-	-	-
36.	संस्थान के लियन कर्मचारियों का एक पद से अन्य पद में स्थानांतरण करना।	पूर्ण शक्तियां व शर्तें वह व्यक्ति संबंधित दोनों पदों पर नियुक्ति प्राप्त करने के लिए प्राधिकृत हैं।	सभी अन्य पदों के लिए पूर्ण शक्तियां	-	-	-
37.	संस्थान के कर्मचारियों का एक पद से अन्य पद में स्थानांतरण करना।	समूह ख, ग और घ कर्मचारियों के मामले में पूर्ण शक्तियां	समूह ख, कर्मचारियों के मामले में पूर्ण शक्तियां	समूह 'क' कर्मचारियों के मामले में पूर्ण शक्तियां	-	-
38.	मूल नियमावली (9) (6) (ख) के अंतर्गत ड्यूटी पर माने गए किसी संस्थान के कर्मचारियों के वेतन और भत्तों का निर्धारण	समूह ख, ग और घ कर्मचारियों के मामले में पूर्ण शक्तियां	समूह 'क' कर्मचारियों के मामले में पूर्ण शक्तियां	-	-	-
39.	वेतन संवर्धन हेतु अतिविशिष्ट अवकाश की गणना	समूह ख, ग और घ कर्मचारियों के मामले में पूर्ण शक्तियां	समूह 'क' कर्मचारियों के मामले में पूर्ण शक्तियां	-	-	-

40.	किसी स्थानापन्न शासकीय कर्मचारी के वेतन में कमी करने की शक्ति	समूह ख, ग और घ कर्मचारियों के मामले में पूर्ण शक्तियां	समूह 'क' कर्मचारियों के मामले में पूर्ण शक्तियां			
41.	मानदेय प्रदान करना और स्वीकृति हेतु मंजूरी देना।	सभी श्रेणी के कर्मचारियों के लिए जारी किए गए मूल नियमावली के नियम 46 (ख) के प्रावधानों और समय-समय पर जारी किए गए भारत सरकार के आदेशों के अनुसार प्रत्येक मामले में प्रतिवर्ष अधिकतम 5000/- रु. तक के लिए पूर्ण शक्तियां। आवृत्ति मानदेयों के ममाले में यह सीमा किसी एक वर्ष में किसी एक व्यक्ति को कुल आवृत्ति भुगतानों के लिए लागू होगी। समूह क और समूह ख कर्मचारियों के मामले में इस मामले की सूचना शासी निकाय को दी जाएगी।	-	-	-	-
42.	किसी कर्मचारी को अस्थायी तौर पर एक से अधिक पद के लिए नियुक्ति और गौण पदों के वेतन तथा आहारित प्रतिपूर्ति भत्ते की राशि का निर्धारण करने की शक्ति।	केंद्रीय सरकारी कर्मचारियों के समान वर्गों के लिए लागू नियमों के अधीन पूर्ण शक्तियां	-	-	-	-

43.	अंशकालिक कर्मचारियों को दी जाने वाले शुल्क की घोषणाकरना (यात्रा भत्ते के उद्देश्य हेतु)	पूर्ण अधिकार प्राप्त				
44.	दो या अधिक वाले तथा छोटे मार्ग तय करने हेतु	पूर्ण अधिकार प्राप्त				
45.	सबसे छोटे अथवा सबसे सस्ते मार्ग के अतिरिक्त माइलेज भत्ते की अनुमति हेतु	पूर्ण अधिकार के द्वारा मार्ग का अपना संसाधन के हित में होगा				
46.	किसी स्थान पर यात्रा के प्रारंभ या अंत का निर्धारण करना	पूर्णअधिकार प्राप्त				
47.	यह घोषित करना कि कोई कर्मचारी जिसका मासिक वेतन 300/- रुपये प्रतिदिन से अधिक ना हो, वह स्टीमर में निवास हेतु पात्र है।	न्यूनतम वर्ग	-	-	-	-
48.	स्टीम निवास की कठिनाई के संदेहास्पद मामले में निर्णय लेना, जिसके लिए संस्थान कर्मचारी योग्य है।	पूर्ण शक्तियाँ				
49.	छुट्टी से लौटने से पहले एक स्वस्थता चिकित्सा प्रमाण पत्र की मांग का अधिकार।	पूर्ण अधिकार प्राप्त	निदेशक के मामले में पूर्ण अधिकार प्राप्त			
50.	अधिक निवास को कवर करने हेतु अवकाश विस्तार	पूर्ण अधिकारों के तहत यह प्रावधान है कि अवकाश प्राप्त कर्मचारी संस्थान के प्रशासनिक नियंत्रण के तहत कार्यभार ग्रहण करेंगे।	अन्य सभी मामलों में पूर्ण अधिकार प्राप्त।	-	-	-
51.	भारत विदेशी सेवाओं में स्थानांतरण की मंजूरी देना और विदेशी सेवा में वेतन का निर्धारण करना	मौलिक तथा प्रतिपूरक नियम खंड 2 के पद तथा टेलीग्राफ पूरक के परिशिष्ट-4 में क्रम संख्या 30 में उल्लिखित कॉलम 4 में वर्णित नियमों के अनुपालन में ख, ग तथा घ समूह के संबंध में पूर्णत: अधिकार प्राप्त।	समूह क कर्मचारियों के संबंध में पूर्ण अधिकार प्राप्त	-	-	-

52.	सरकारी कर्मचारी के प्रत्यावर्तन की तिथि निर्धारित करना जिसने विदेशी सेवा से पहले अवकाश लिया हो। तारीख तय करना जो विदेशी सेवा से प्रत्यावर्तन से पहले छुट्टी लेता है	पूर्ण अधिकार-प्राप्त	-	-	-	-
53.	सौंपे गए कार्य हेतु शुल्क की स्वीकृति की शक्ति तथा उस शुल्क की स्वीकृति ।	पूर्ण अधिकार-प्राप्त	-	-	-	-
54.	नियमों की छूट देते हुए अधिकारियों की हवाई यात्रा	आपातकालीन तथा आवश्यकता के मामले में पूर्ण अधिकार-प्राप्त।	-	-	-	-
55.	सड़क माध्यम की सभी यात्राओं की क्षतिपूर्ति सहित संस्थान कर्मचारी के वेतन का भुगतान	समूह क, ख और ग समूह के मामलों में पूर्ण अधिकार प्राप्त	समूह क कर्मचारियों के मामले में पूर्णत: अधिकार-प्राप्त			
56.	दस दिनों के लिए दौरे पर रोक को सीमित करने वाले नियम से छूट देने की शक्ति।	30 दिनों की सीमा तक पूर्ण शक्तियां	30 दिनों से अधिक तक की अवधि तक पूर्ण अधिकार प्राप्त	-	-	-
57.	संस्थान द्वारा कर्मचारी को यात्रा हेतु किराए तथा शुल्क राशि निर्धारण करने का अधिकार तथा इसके लिए सभी प्रकार की लागत का भुगतान ।	पूर्णत: अधिकार प्राप्त				
58.	जांच समिति में भाग लेने वाले गैर-अधिकारियों को यात्रा भत्ता देना तथा उनके ग्रेड निर्धारित करना।	पूर्णत: अधिकार प्राप्त	-	-	-	-
59.	नियंत्रित अधिकारी की घोषणा करना तथा उनके दिशानिर्देश हेतु नियम बनाना	कोई भी संस्थान अपने नियंत्रण अधिकारी की घोषणा नहीं कर सकता।	-	-	-	-
60.	विशेष अयोग्यता अवकाश के अतिरिक्त अवकाश प्रदान करना।	पूर्णत: अधिकार प्राप्त				
61.	जब कोई चिकित्सा बोर्ड यह रिपोर्ट देता है कि कोई व्यक्ति कार्यभार संभालने के संदर्भ में उपयुक्त नहीं है, उसे अवकाश प्रदान करना।	पूर्णत: अधिकार प्राप्त	-	-	-	-

62.	किसी विशेष मामले में यह निर्णय लेना कि क्या कोई विशेष कर्मचारी किसी रिक्त विभाग में कार्यरत है अथवा नहीं।	पूर्णत: अधिकार प्राप्त	-	-	-	-
63.	मातृत्व तथा अस्पताल अवकाश प्रदान करना	पूर्णत: अधिकार प्राप्त	-	-	-	
64.	यात्री की सामान्य यात्रा के अतिरिक्त कार्यभार ग्रहण करने के समय की गणना हेतु मंजूरी प्रदान करना	पूर्णत: अधिकार प्राप्त	-	-	-	-
65.	कार्यभार ग्रहण करने के समय में 30 दिनों की अधिकतम अवधि तक विस्तार करना	पूर्णत: अधिकार प्राप्त	तीस दिनों से अधिक हेतु भी पूर्णत: अधिकार प्राप्त	-	-	-
66.	संस्थान के कर्मचारी को देश के किसी भी हिस्से में जाकर उसको कार्य करने की अनुमति प्रदान करना		समूह 'क' के कर्मचारियों के मामले में पूर्ण अधिकार प्राप्त	-	-	-
67.	कर्मचारियों की सेवा रोल में जन्म तिथि की क्लर्क संबंधी गलतियों में सुधार।	समूह 'ग' और "घ" कर्मचारियों के मामले में पूर्णत: अधिकार प्राप्त	समूह 'क' और "ख" कर्मचारियों के मामले में पूर्णत: अधिकार प्राप्त	-	-	-
68.	3 वर्ष से कम तथा 6 वर्ष से अधिक बकाया के भुगतान के दावों की जांच की मंजूरी के अधिकार।	पूर्णत: अधिकार प्राप्त	अन्य मामलों में पूर्णत: अधिकार प्राप्त।	-	-	-
69.	निदेशक के अतिरिक्त अन्य कर्मचारियों के संबंध में स्थाई स्कीम के भुगतान की मंजूरी।	पूर्णत: अधिकार प्राप्त	निदेशक के मामले में पूर्णत: अधिकार प्राप्त	-	-	-
70.	आकस्मिक व्यय के मामले में अधीनस्थ प्राधिकारियों को निदेश जारी करने के अधिकार।	पूर्णत: अधिकार प्राप्त	-	-	-	-
71.	अप्रचलित अधिशेष तथा अप्रतिरोहय स्टोर का निष्कासन।	पूर्णत: अधिकार प्राप्त	-	-	निदेशक, कंडमनेशन बोर्ड जो संस्थान द्वारा गठित इस प्रयोजन के लिए है की सलाह पर कार्य करेगा।	
72.	अन्य मामलों में संस्थान के कर्मचारियों का अग्रिम भुगतान की शर्तों का बदलने का अधिकार।	उन मामलों में जहां निदेशक अनुदान की स्वीकृति हेतु सक्षम है वहां ब्याज वाले अग्रिम भुगतान की वृद्धि में विस्तार नहीं किया जा सकता।	अन्य सभी मामले	-	-	-

73.	वाहन खरीदने के लिए अग्रिम की मंजूरी।	सामान्य वित्त नियम के 2018 के नियम 199 में निर्धारित शर्तों तथा नियमों के अनुपालन में संस्थान में स्थाई पदों के कर्मचारियों के मामले में पूर्ण अधिकार।	-	-	-	-
74.	संस्थान से प्राप्त अग्रिम से खरीदे गए वाहनों की बिक्री तथा हस्तांतरण करने का अधिकार।	सामान्य वित्त नियम के नियम-256 के खंड (2) में वर्णित मामलों में पूर्ण अधिकार।	-	-	-	-
75.	साईकिल की खरीद हेतु दिए गए अग्रिम की अधिकतम 24 किश्तों से अधिक किश्तों का पुन: भुगतान संस्थान को करने का अधिकार।	पूर्णत: अधिकार प्राप्त				
76.	यात्रा, स्थानांतरण हेतु संस्थान कर्मचारियों को अग्रिम राशि की मंजूरी का अधिकार	सामान्य वित्त नियमों के नियम 234 के 231 में निर्धारित शर्तों के आधार पर सरकार में स्थाई तथा अस्थाई कर्मचारियों के मामले में पूर्ण अधिकार।	-	-	-	-
77.	उस संस्थान को मुकदमें के लिए अग्रिम स्वीकृत करने की शक्ति जिसमें संस्थान एक पक्षकार है।		-	-	-	-
78.	रोकड़, भंडार आदि रखने वाली अधीनस्थ प्राधिकरण द्वारा निष्पादित किए जाने वाले सुरक्षाबंद पत्र अवधि निर्धारित करने की शक्ति।	पूर्णत: अधिकार प्राप्त	-	-	-	-
79.	ट्रेजरी नियमावली के तहत महत्वपूर्ण त्योहारों को अग्रिम राशि के भुगतान करने की शक्ति।	पूर्णत: अधिकार प्राप्त	-	-	-	-
80.	संस्थान के धन की सुरक्षा से संबंधित नियम 109(i) के प्रावधानों के तहत प्रस्थान की शक्ति।	पूर्णत: अधिकार प्राप्त		-	-	-

अनुसूची II
(विनियमन 33 देखें)

संस्थान में विभिन्न पदों हेतु नियुक्ति, अनुशासनात्मक तथा अपीलीय प्राधिकारी

क्र.सं.	पद का विवरण	नियुक्त प्राधिकारी	केंद्रीय सिविल सेवा (वर्गीकरण नियंत्रण और अपील) प्राधिकरण 1965 के नियम-11, संदर्भ में सक्षम प्राधिकारी द्वारा दंड दिया जा सकता है।		अपीलीय प्राधिकारी
			अनुशासनात्मक प्राधिकरण	केन्द्रीय सिविल सेवाएं (वर्गीकरण, नियंत्रण तथा अपील) नियम, 1965 के नियम-11 के तहत दंड	
1	2	3	4	5	6
1	समूह 'क' पद (i) निदेशक	अखिल भारतीय आयुर्विज्ञान चिकित्सा संस्थान नियम - 7	संस्थान	सभी केन्द्रीय सरकार के पूर्वानुमोदन से (v) से (ix) दंड नहीं दिए जा सकते।	
	(ii) अन्य पद	शासकीय निकाय	(क) शासी निकाय (ख) अध्यक्ष	(क) सभी दंड (ख) (i) से (iv) दंड	(क) संस्थान शासकीय निकाय
2	समूह 'ख' के पद	अध्यक्ष	(ग) अध्यक्ष (घ) निदेशक	(ग) सभी दंड (घ) (i) से (iv) दंड	(ख) शासी निकाय (ग) अध्यक्ष
3	समूह 'ग' के पद	निदेशक	(क) निदेशक	(क) सभी दंड	(क) अध्यक्ष
4	समूह 'घ' के पद	निदेशक	(क) निदेशक (ख) उप निदेशक (प्रशासन) निम्न (ग) तथा (घ) में दिए गए कर्मचारियों के अतिरिक्त संस्थान के कर्मचारियों के मामले में (ग) अखिल भारतीय चिकित्सा विज्ञान के मामले में चिकित्सा अधीक्षक (घ) मुख्य संयोजक, डॉ. राजेंद्र प्रसाद नेत्र रोग विज्ञान केंद्र तथा संबद्ध केंद्रों में कार्यरत कर्मचारियों के मामले में संस्थान द्वारा स्थापित अन्य केन्द्र।	(क) सभी दंड (बी) जुर्माना (i) से (iv) (ग) (i) से (iv) दंड (घ) (i) से (iv) दंड	(क) अध्यक्ष (ख) निदेशक (ग) निदेशक (घ) निदेशक

(i) अखिल भारतीय आयुर्विज्ञान संस्थान के अध्यक्ष शासकीय निकाय के अनुमोदन प्राप्त होने पर चार्जशीट, दोषारोपण के विवरण, दंड तथा आदेशों का स्थगन हेतु अखिल भारतीय आयुर्विज्ञान संस्थान के निदेशक की प्राधिकृति अथवा जैसा भी मामला हो। सूचना, चार्जशीट तथा दोषारोपण के विवरणों पर शासकीय निकाय अथवा अध्यक्ष की ओर से निदेशक द्वारा हस्ताक्षर होने चाहिए अथवा जो भी मामला हो तथा इन दस्तावेजों में यह तथ्य उल्लिखित होना चाहिए। इन दस्तावेजों पर "अध्यक्ष निकाय के आदेश द्वारा" अथवा "अध्यक्ष" अथवा "शासकीय निकाय अनुमोदन से" अथवा "अध्यक्ष" जैसे वाक्यांशों का उपयोग किये जा सकते हैं।

(ii) चूंकि शासकीय निकाय की बैठकें अंतराल पर आयोजित की जाती हैं, इसलिए 'क' समूह के कर्मचारियों तथा संकाय सदस्यों के विरुद्ध अनुशासनात्मक कार्रवाई आरंभ करने हेतु शासकीय निकाय के अध्यक्ष प्राधिकृत हैं तथा दंड पर अंतिम निर्णय शासकीय निकाय की बैठक में लिया जाएगा।

संस्थान के प्राधिकार द्वारा

रणदीप गुलेरिया, निदेशक

[विज्ञापन–III/4/असाधारण/248/19]

MINISTRY OF HEALTH AND FAMILY WELFARE

(ALL INDIA INSTITUTE OF MEDICAL SCIENCES)

NOTIFICATION

New Delhi, the 18th October, 2019

F. No. 14-3/69(98)/Coordination Cell/Estt.(Part-II) .— In exercise of the powers conferred by sub-section (1) of section 29 of All India Institute of Medical Sciences Act, 1956 (25 of 1956) and in supersession of the All India Institute of Medical Sciences Regulations, 1999, except as respects things done or omitted to be done before such supersession, the Institute with the previous approval of the Central Government hereby makes the following regulations, namely:—

1.	**Short title and commencement.** —(1)These regulations may be called the All India Institute of Medical Sciences Regulations, 2019. (2)They shall come into force on the date of their publication in the Official Gazette.
2.	**Definitions.** — (1) In the regulations, unless the context otherwise requires, — (a) "Act" means the All India Institute of Medical Sciences Act, 1956 (25 of 1956); (b) "Chairman" means the Chairman of the Governing Body under sub-section (3) of section 10 of the Act; (c) "Deputy Director" means the Deputy Director (Administration) of the Institute; (d) "Director" means the Director of the Institute appointed under sub-section (1) of section 11 of the Act: (e) "Fundamental Rules" means the fundamental rules as applicable to Central Government Servants; (f) "General Financial Rules" means the General Financial Rules, 2017 framed and as amended from time to time by the Central Government for financial management and control; (g) "President" means the President of the Institute nominated by the Central Government under sub-section (1) of section 7 of the Act; (h) "Rules" means the rules framed by the Central Government under sub-section (1) of the section 28 of the Act; (i) "Schedule" means a Schedule annexed to these regulations; (j) "Secretary" means a Secretary of the Institute and the Governing Body; (k) "Supplementary Rules" means the Supplementary Rules as applicable to Government servants who are subject to the Fundamental Rules; (l) "Treasury Rules" means the Treasury Rules of the Central Government.

	(2) Words and phrases used in these regulations and not defined but defined in the Act shall have the meanings respectively assigned to them.
3.	**Powers and Functions of the President.**—The President shall exercise such powers and discharge such functions as are laid down in the Act, the rules and these regulations including Schedule I.
4.	**Meetings of the Institute.**— (1) The Institute may meet as often as may be considered necessary by the President for the transaction of the business of the Institute but shall meet at least twice a year. (2) (a) Meeting of the Institute shall be held at the date and time as may be fixed by the President. (b) The Proceedings of the meeting shall be circulated to all the members of the Institute by the Director after obtaining the approval of the President and a period of seven days will be given to the members to confirm the proceedings. (c) All proceedings of meetings of the Institute shall be entered in a Minutes Book to be maintained by the Secretary for the purpose and each minute shall be signed by the President of that meeting after the same is duly confirmed by the member present. (3) For a ordinary meeting of the Institute a notice specifying the place, date and time of the meeting shall be given by the Secretary to the members at least two weeks prior to the date of such meeting either electronically or by speed post. The agenda shall also be sent alongwith the notice of the meeting and where it is not possible, the agenda shall be sent at least ten days before the meeting either electronically or by speed post. (4) An extraordinary meeting of the Institute may be called by the President at any time for the transaction of urgent business of the Institute. (5) For extraordinary meetings, notices specifying the place, date and time of the meeting shall be sent by the Secretary to the President and the members at least five days before the date of the meeting, under a certificate of posting, if sent by post, or by electronically or by speed post. The agenda shall be sent either electronically or by speed post, at least three days before the meeting. (6) An extraordinary meeting of the Institute may be called on a written request of not less than nine members of the Institute within seven days of the receipt of the requisition and the request made by members requisitioned meeting shall indicate the purpose of the meeting. (7) In the absence of the President at any meeting of the Institute, the members present shall elect a person from among themselves to preside over such meeting. (8) The quorum for a meeting of the Institute shall be seven. (9) The President may include in the agenda at any time before or during a meeting (i) fresh items of business; (ii) items supplementary to those included in the agenda; and such items shall also be taken up for consideration. (10) Any member desirous of moving any resolution at a meeting of the Institute shall give notice thereof in writing to the Secretary so as to reach him not less than fourteen days before the date of the meeting. When such notice has been given, the proposed resolution shall be circulated immediately by the Secretary to the members and be included in the agenda. (11) Members can also participate in the meeting through video conference, after obtaining the prior approval of the Chairman and such participation through video conference will be counted for the purpose of the quorum. (12) If any non-official member nominated to the Institute does not participate in three consecutive meetings of the Institute or Governing Body or Standing Committees without any valid reason to the satisfaction of President, his membership shall be terminated with the approval of the President. (13) No subject disposed of by the Institute at a meeting shall be brought up again for consideration until after the expiry of one year except in a case where the President or Government certifies that the subject required further consideration in the interest of the Institute. (14) A decision given by the President of the meeting on a point of order raised by a member shall be final. (15) All decisions of the Institute shall be taken on a majority vote and in case of equality of votes the President shall have a casting vote. (16) Any business of the Institute may be transacted by circulation of papers to the members and the President and acted upon, if unanimously approved. The resolution and the action taken thereon shall be placed before the next meeting of the Institute for confirmation.
5.	**Constitution of the Governing Body.** —The Governing Body shall consist of the following eleven members, namely: - (a) President of the Institute. — Chairman; (b) Director General of Health Services. — Ex-Officio Member;

	(c) Representative of the Ministry of Finance. (d) Director, All India Institute of Medical Sciences. (e) One member elected by the members of the Institute from amongst the three members of the Parliament elected to the Institute. (f) Six members to be elected by the members of the Institute from amongst themselves. (g) Following permanent Special Invitees: - (i) Additional Secretary (in the Ministry of Health and Family Welfare in charge of the Institute); (ii) Joint Secretary (in the Ministry of Health and Family Welfare in charge of the Institute); (iii) Dean (Academics); (iv) Deputy Director (Administration.); (v) Senior Financial Advisor.	Ex Officio Member; Member
6.	**Powers and functions of Governing Body.**—The Governing Body shall exercise such powers and discharge such functions as are laid down in these regulations including Schedule I.	
7.	**Powers and functions of Chairman.**—The Chairman shall exercise such powers and discharge such functions are laid down in these regulations.	
8.	**Meetings of Governing Body.**—(1) The Governing Body may meet as often as may be considered necessary by the Chairman for transaction of its business, but shall ordinarily meet at least thrice a year preferably in the month of January, May and September. (2) The proceedings of the meeting shall be circulated to the members of the Governing Body by the Director after obtaining the approval of the Chairman. A period of fourteen days will be given to the members to confirm the proceedings. (3) All Proceedings of meetings of the Governing Body shall be entered in a Minute Book to be maintained by the Secretary for the purpose and all minutes shall be signed by the Chairman of the meeting after the same is duly confirmed by the members present. (4) An extraordinary meeting of the Governing Body shall be called on a written requisition by at least six members of the Governing Body or by the Chairman. (5) Notice of every meeting of the Governing Body shall be sent by the Secretary to the members of the Governing Body, in the case of an ordinary meeting at least fourteen days and in the case of an extraordinary meeting at least seven days, before the date of the meeting either electronically or by speed post under certificate of posting when sent by post. The agenda of meetings shall be sent under certificate of posting if sent by post or electronically or by speed post at least ten days and five days respectively, before the date of the meeting. (6) In the absence of the Chairman at any meeting, the members present shall elect a person from amongst themselves to preside at the meeting. (7) Five members shall form the quorum, members can also participate in the meeting through video conference, after obtaining the prior approval of the Chairman and such participation through video conference will be counted for the purpose of the quorum. (8) All decisions of the Governing Body shall be taken by a majority vote. In case of equality of votes the chairman shall have a casting vote. (9) Any member desirous of moving any resolution at a meeting of the Governing Body shall given notice thereof in writing to the Secretary so as to reach him not less than seven days before the date of such meeting. Such notice when received shall be circulated immediately by the Secretary to the members and be included in the agenda of the meeting. (10) Any matter not included in the agenda and of which the notice mentioned in sub- regulation (9) has not been given may be considered at a meeting of the Governing Body with the permission of the Chairman. (11) Any business of the Governing Body may be transacted by circulation of papers to the members and Chairman and acted upon if unanimously agreed to. The decision and the action taken thereon shall be placed before the next meeting of the Governing Body for confirmation. In case the resolution is not confirmed by the Governing Body in the next meeting, the action already taken in compliance of the resolution circulated and agreed to by the members shall be valid. (12) If a non-official member nominated in the Governing Body remains absent in three consecutive meetings without any valid reason, his membership shall be terminated with the approval of the Chairman.	
9.	**Terms of office of members of Governing Body.** —(1) The term of office of a member other than an ex-office	

	member of the Governing Body shall be five years subject to his continuance as a member of the Institute and an out-going member shall be eligible for re-election. (2) Casual vacancies of elected members shall be filled by election by the Institute for the remaining period of the vacancy.
10.	**Allowance to the Chairman and members of the Governing Body, standing committee and ad-hoc committee.**—(1)The Chairman and the members of the Governing Body, the Standing Committees, and ad-hoc committees shall not receive any pay, fee, remuneration or other allowance except travelling and daily allowance for attending meetings. (2) The Chairman and the members of the Governing Body and of the standing and ad-hoc committees, if they are officers of the Central or a State Government shall be paid travelling and daily allowances by the Institute at the rate admissible to them as officers of the Central or the State Government. (3) In the case of Chairman and the members of the Governing Body and of standing and ad-hoc committees other than those mentioned in sub-regulation (2), travelling allowance and daily allowance shall be paid at the rates to which they are entitled as per rules of the organisation in which they are working or those prescribed from time to time by the Central Government under Supplementary Rules and the executive decision and orders there under, whichever is more. (4) The President may, for special reasons, sanction journeys by air not otherwise admissible by members of the Governing Body and of Standing and ad-hoc committee for such journeys travelling allowance shall be paid at rates admissible to Group 'A' officers of the Central Government.
11.	**Powers and duties of Director.** —The Director shall be the Head of Institute in terms of sub-rule (10) of rule 2 of the Supplementary Rules and shall exercise the powers of Head of Institute and discharge the following duties, namely: - (a) he shall be in-charge of the administration of the Institute. He shall allocate duties to the officers and employees of the Institute and shall exercise such supervision and executive control as may be necessary subject to the rules and these regulations; (b) he shall exercise the powers specified in Schedule I to these regulations; (c) he shall have the powers to delegate any of his powers to the officers on the administrative side subject to such limitations as may be imposed by the Governing Body.
12.	**Procedure in conducting business of Standing Committees.** — (1) All standing committees shall be advisory committees. (2) Fifty per cent of the members shall form the quorum for all standing committee. Members can also participate in the meeting through video conference, after obtaining the prior approval of the Chairman and such participation through video conference will be counted for the purpose of the quorum. In the case of Standing Selection Committee or Combined Selection Committee or Regional selection Committee, the two experts shall also be counted for purpose of determining the quorum.
13.	**Building and lands belonging to the Institute.**— (1) The Institute shall use its lands and buildings for the purposes of the Institute. (2) The allotment and the assessment and recovery of rent of buildings shall as far as may be made by the Director in accordance with the provisions of rules 45A, 45B and 45C of Fundamental Rules and the Supplementary Rules. (3) Every employee of the Institute, if offered residential accommodation in the premises of the Institute shall stay in that residence and pay thereof such rent and other charges as may be fixed by the Institute.
14.	**Powers to award prizes, scholarships.**—The Institute may award such prizes, souvenirs, stipends and scholarships to its students as may be decided by the Governing Body from time to time.
15.	**Procedure for appointment of Dean and Associate Dean.**— (1) There shall be three Deans, namely, Dean (Academic), Dean (Research) and Dean (Examination). A Professor and Head of Department shall be appointed as Dean by the Institute taking into consideration the seniority in consultation with the Director. (2) There shall be three Associate Deans, namely, Associate Dean (Academic), Associate Dean (Research), and Associate Dean (Examination). Any faculty (Additional Professor or above) can be appointed as Associate Dean by the Institute in consultation with Director. The Associate Dean (Academic) and Associate Dean (Research) shall be appointed from medical faculty only. (3) The tenure of the Dean and Associate Dean shall be for a maximum period of three years and further extendable for one more term by the Institute in consultation with Director of the Institute. (4) The Deans and Associate Deans shall be appointed from existing faculty members and no additional remuneration shall be paid unless as approved from time to time by the Government of India.
16.	**Professorships.**—The Institute may create and appoint persons to Professorships, Additional Professorships, Associate Professorships, Assistant Professorships, Lectureships, Professor cum Principal to College of Nursing, Professor cum Vice Principal to College of Nursing, Associate Professor in Nursing, assistant professor in Nursing and other posts. No post shall be created without the approval of the Government of India.
17.	**Power to arrange lectures.** —The Institute may invite experts to deliver lectures in the Institute from time to

	time on payment of suitable fees or honoraria and pay them travelling allowance at the rates admissible to Central Government employees of similar status for their journey within India.
18.	**Fee and other charges**. —All fee and other charges payable by the candidates selected for admission to various courses of Institute shall be as recommended by Academic Committee and approved by the Standing Finance Committee, Governing Body and Institute from time to time.
19.	**Admission to courses of studies**.—The reservation for the Scheduled Castes (SC), Scheduled Tribes(ST), Other Backward Classes(OBC), Economically Weaker Sections (EWS) and other categories shall be as per policy laid down by the Government of India from time to time.
20.	**Award of degrees**.—The Institute may grant MBBS, MD, MS, Ph-D, DM, M.Ch, MHA, MDS, Fellowship, M.Sc, M. Biotech, B.Sc. (Honours) Human Biology, B.Sc. (Honours) Nursing, B.Sc. Nursing (Post-certificate), B.Sc. (Honours) in paramedical subjects and any other degrees as the Institute may consider desirable with the approval of Standing Academic Committee of the Institute and ratification by the Governing Body .
21.	**Conduct of examination (academic as well as recruitment).—**Such number of supervisors, invigilators, examiners (internal or external) and other staff as may be necessary for conducting the examination, paper setting, examination of answer books or thesis, oral and practical of the Institute, may be appointed by the Director and paid remuneration, as recommended by the Academic Committee and approved by the Standing Finance Committee, Governing Body and the Institute from time to time.
22.	**Whole time Employees**.—Unless, in any case, otherwise it is distinctly provided, the whole time of an employee of the Institute shall be at the disposal of the Institute and he may be employed in any manner as required by the proper authority of the Institute without claim for additional remuneration.
23.	**Permanent and Temporary Posts.**— (1) The posts in the service of the Institute shall be permanent post that is a post carrying a definite rate of pay sanctioned without any limit of time or a temporary post that is a post carrying a definite rate of pay sanctioned for a limited time. A person occupying a permanent post, on appointment to a higher position for a specified period, shall be allowed to retain his lien in the previous post initially for a maximum of five years, extendable for two years or premature repatriation. (2) Temporary posts of Resident Doctors shall be governed by the Residency Scheme of the Ministry of Health and Family Welfare in the Government of India as modified from time to time.
24.	**Qualifications for appointment**. — (1) Age, experience and other qualifications for appointment to a post under the Institute shall be prescribed by the appointing authority keeping in view the qualifications and experience prescribed by the Central Government for similar posts before applications of candidates are called for subject to the condition that non-medical personnel shall not be appointed to the post of Director to be notified separately from time to time after approval of the appointing authority. (2) The Director shall, in filling vacancies in posts and services, under the Institute, make such reservations, in favour of the Scheduled Castes, Scheduled Tribes, Other Backward Classes, Economically Weaker Sections and other categories as may be made by the Central Government from time to time, in filling vacancies in posts and services under the Central Government.
25.	**Period of probation**.—Unless otherwise decided by the appointing authority in any case, all employees shall be on probation for two years. During the period of probation, the employee shall be required to put in satisfactory service failing which his services shall be liable to termination at any time without any notice or reason being assigned for the same. The appointing authority may, however, extend the period of probation.
26.	**Seniority**.— The seniority of employees of the Institute in each category shall be determined by the order of merit in which they were selected for appointment to the post in question, those selected on an earlier occasion being ranked senior to those selected later.
27.	**Leave**.— (1) Temporary and permanent employees of the Institute shall be entitled to such leave and leave salary as are admissible to the corresponding categories of the Central Government servants under the Central Civil Services (Leave) Rules, 1972: Provided that for the purpose of the Central Government Central Civil Services (Leave) Rules, 1972, the following categories of teaching staff in the Institute or any other post declared as academic post by the standing academic committee and ratified by the Governing Body from time to time shall be treated as serving in the vacation Department, namely:- (1) Professor, (2) Additional Professor, (3) Associate Professor, (4) Assistant Professor, (5) Medical Superintendent, (6) Additional Medical Superintendent, (7) Principal, College of Nursing, (8) Lecturers in Nursing, (9) Senior Nursing Tutors, and (10) Tutors in Nursing: (2) The regular vacation for the purpose shall be as may be decided by the Governing Body from time to time:

	Provided that an incumbent on deputation to the Institute as on foreign service shall be governed by the leave rules as may be stipulated in the conditions of their deputation.
28.	**Pension and Contributory Provident Fund.**— (1)The employees of the Institute, except those on deputation on foreign service to the Institute, appointed on or after 12th September, 1975 and such employees as were appointed prior to this date but have specifically opted for the General Provident Fund and pensionary benefits as applicable to the Central Government employees shall be governed by the provisions of the General Provident Fund (Central Services) Rules, 1960 and the Central Civil Services (Pension) Rules, 1972. (2) With effect from 1st January, 2004, the date on which the New Pension Scheme was introduced, all new entrants who joined the service of the Institute on or after 1st January, 2004, shall be governed by the New Pension Scheme.
29.	**Absence from duty. —** Unless otherwise decided by the President in exceptional circumstances, no permanent employees of the Institute shall be away from his post, otherwise than on leave or because of suspension, for periods and purposes stated in the guidelines approved in this regard from time to time by the Governing Body.
30.	**Superannuation. —** (1) The age of superannuation of an employee of the Institute other than teaching faculty shall be sixty years or as specified by the Government of India from time to time: Provided that the scientific specialists may be granted extension in service, on a case to case basis upto the age of sixty-two years in the case of persons who are exceptionally talented for reasons to be recorded in writing and subject to physical fitness and continued efficiency of the person concerned. (2) The age of superannuation of a member of the teaching faculty of the Institute shall be sixty-five years or as specified by the Government of India from time to time. (3) Notwithstanding anything contained in sub-regulations (1) and (2), the appointing authority shall be of the opinion that it is in the public interest so to do, have the absolute right to retire any employee of the Institute by giving him a notice of not less than three months in writing or three months pay and allowances in lieu of such notice — (i) if he is in Group A or Group B service or post and had entered the service of the Institute before attaining the age of thirty-five years, after he has attained the age fifty years; and (ii) in any other case, after he has attained the age of fifty-five years: Provided that nothing in this sub-regulation shall apply to an employee in Group D service or post who entered the service on or before the 1st December, 1962 (4) Any employee of the Institute may, by giving notice of not less than three months in writing to the appointing authority, retire from the service after he has attained the age of fifty years, if he is in Group A or Group B service or post and had entered the service of the Institute before attaining the age of thirty-five years, and in all other cases after he has attained the age of fifty-five years: Provided that, — (a) nothing in this sub-regulation shall apply to an employee in Group D service or post who entered service on or before the 1st December, 1962; (b) it shall be open to the appointing authority to withhold permission to an employee under suspension who seeks to retire under this sub-regulation. ***Explanation***.–In this regulation the expression "member of the teaching faculty" means the Professor, Additional Professor, Associate Professor, Assistant Professor, Medical Superintendent, Additional Medical Superintendent, Principal of College of Nursing, Lecturer in Nursing, Senior Nursing Tutor and Tutor in Nursing and other employees of the Institute as may be declared to be members of the teaching faculty by the Central Government from time to time.
31.	**Term of office of Director. —**(1)The Director shall have a term of five years from the date of assumption of charge of the post or till he attains the age of sixty-five years, whichever is earlier. (2) Notwithstanding anything contained in these regulations, the Institute shall, if it is of the opinion that it is in the public interest to do so, have the right to terminate the term of office of Director at any time before the expiry of his term by giving him a notice of not less than three months in writing or three months salary and allowances in lieu thereof. The Director shall also have the right to relinquish his office at any time before the expiry of the fixed term by giving to the Institute a notice of not less than three months in writing.
32.	**Age at recruitment**. —The maximum age of a candidate at the time of recruitment to the service of the Institute shall normally be fifty years for teaching posts and thirty years for non teaching posts or as indicated in the recruitment rules for each post (except for Senior Demonstrators or Senior Residents in all Departments of the All India Institute of Medical Sciences where it shall be thirty-three years or as recommended by the Standing Academic Committee from time to time). This limit is relaxable by the Governing Body.
33.	**Conduct, discipline and penalties. —**(1)The Central Civil Services (Conduct) Rules, 1964 as modified from time to time, shall apply to the employees of the Institute.

	(2) Part IV (Suspension), Part V (Penalties and Disciplinary Authorities) Part VI (Procedure for imposing penalties), Part VII (Appeals) and Part VIII (Review) of the Central Civil Service (Classification, Control and Appeal) Rules, 1965 as modified from time to time, shall apply to the employees of the Institute: Provided that for the purpose of this regulation, — (a) Group A, Group B, Group C and D post in the Institute shall correspond to the Central Civil Services Group A, Group B, Group C and Group D post respectively; (b) the Appointing Authority, the disciplinary Authority for the penalties that may be imposed and the Appellate Authority for the various posts in the Institute shall be as prescribed in Schedule II; (c) in respect of Central or State Government servants borrowed by the Institute, the provision respectively of rules 20 and 21 of the Central Civil Services (Classification, Control and Appeal) Rules, 1965 shall apply and the Institute shall exercise the functions of the Central or State Government, as the case may be, for the purpose of these rules; (d) no consultation with the Union Public Service Commission shall be necessary in any case.
34.	**Medical facilities for employees.**—(1) The employees of the Institute including deputationists and members of their families shall be entitled to medical aid as admissible under the All India Institute of Medical Sciences Staff Health Scheme. They shall also pay such contribution as are required under that Scheme. (2) In the case of retired employees of the Institute and members of their families as well as those employees and their family members who avail medical facilities in places other than the place of the Institute, the Central Services Medical Attendants Rules, 1944 as amended from time to time, shall apply. In case of any difficulty, the re-imbursement of medical expenses incurred in such cases be done as per applicable rates of Central Government Health Scheme.
35.	**Other conditions of service**. —In respect of matters not provided for in these regulations, the rules as applicable to the Central Government servants regarding the general conditions of service, pay, allowances including travelling and daily allowances, leave salary, joining time, foreign service terms and orders and decisions issued in this regard by the Central Government from time to time shall apply to the employees of the Institute.
36.	**Allotment of Institute residence to employees.**—The employees of the Institute shall be entitled to the allotment of residences at the All India Institute of Medical Sciences in accordance with the provisions laid down by the Institute from time to time.

SCHEDULE I

(See regulations 3, 6 and 11)

Extent of Powers

Sl. No.	Nature of Powers	Director	President	Governing Body	Institute	Remarks
(1)	(2)	(3)	(4)	(5)	(6)	(7)
1.	Powers of re-appropriation of funds from sanctioned budget	Full Powers	-	-	-	Report of any re-appropriation shall be placed before the Governing Body for approval in its subsequent meeting.
2.	(a) (i) Write off of loss of irrecoverable value of stores of public money due to fraud.	Up to Rs. 2,000/-in each case	Rs. 10,000/- in each case	Rs. 20,000/- in each case	Full powers	
	(b) Loss of revenue or of irrecoverable advance					
	(c) Deficiencies and depreciation in value of stores					

3.	To incur (i) contingent expenditure, or (ii) expenditure on the purchase of stores and stationery and printing of forms.	Full powers within the sanctioned budget.	-	-	-	-
4.	Maintenance of Building and petty works:–	--		-	-	-
	(a) Original works and special repairs	Rs.20,000/ in each case subject to maximum of Rs. One lakh per year	Rs. 50,000/- in each case subject to maximum of Rs. 2. 5 lakh per year	-	-	-
	(b) Ordinary repairs	Full powers for minor repairs (not annual repairs)	-	-	-	-
	(c) Annual repairs	Full powers	-	-	-	-
5.	Power to sanction recoverable advances	Full powers in respect of all officers and employees except himself	In case of Director	-	-	-
6.	Power to sanction advances/Final withdrawal out of the Contributory/ General Provident Fund	Full Powers in respect of all officers and employees except himself	In case of Director	-	-	-
7.	Destruction of official records connected with accounts	Full powers subject to the conditions laid down in Appendix 13 to the General Finance Rules	-	-	-	-
8.	Power to direct the payment on the last working day of a month that the pay and allowances of employees of the Institute's where the first four day of the following month are public holiday	Full powers	-	-	-	-
9.	Power to order the retention of undisbursed pay and allowances of establishment for any period not exceeding three months	Full powers	-	-	-	-
10.	To allow mileage allowance by a route other than the shortest or the cheapest	Full Powers provided selection of the route is in Institute's interest.	-	-	-	-

11.	To permit Group 'D' employees to draw next higher class Railway fare when accompanying an officer on train which provides No. II class	Full powers				
12.	To decide whether a particular absence is absence on duty within the country	Full powers for academic purposes and one monthin other cases	Full powers beyond onemonth in all cases other than academic	-	-	-
13.	To impose restrictions on the exchange of daily allowances mileage allowance by Group 'C' and Group 'D' employees, travelling in a public or hired conveyance.	Full powers				
14.	To countersign his own travelling allowance bills and those of other employees	Full powers	-	-	-	-
15.	To waive provision (s) to Supplementary Rule 209 and to authorise departures from Supplementary Rule 211 regarding combination of holidays with leave.	Full powers	-	-	-	-
16.	(i)Grant of Casual Leave	Full powers	Casual Leave of the Director.	-	-	-
	(ii)Grant of Leave	Full powers for Group B , C, D, and not more than four weeks for Group A	Full powers for Group 'A' for more than four weeks and full powers in the case of the Director	-	-	-
	(iii)Special disability leave			Full powers	-	-
17.	To direct that an officer on leave shall be considered to be in occupation of a residence	Full powers for the period of original deputation or the period of leave sanctioned	-	Full powers	-	-

18.	To allot residence	Full powers	-	-	-	-
19.	Power to make appointments to posts subject to rule 7 of the All India Institute of Medical Sciences Rules, 1958.	Full powers	-	-	-	-
19	(i) Ad-hoc/ Temporary	Full powers for Group B, C, & D posts lecturers Assistant Professors and Associate Professors not exceeding a period of one year.	Full power for all Group 'A' posts other than Faculty posts. Professor and Additional Professor for a period not exceeding one year and Lecturers, Assistant Professor and Associate Professor for a period exceeding one year.	-	-	-
	(ii) Permanent	Group C and D post	Group B posts	Group A posts	-	-
20.	Power to confirm Group A & B officers, after successful completion of the period of probation.	Full powers except in the case of the Director	-	-	-	-
21.	Power to accept resignation of Group Demployees	Full powers	-	-	-	-
22.	Powers to accept resignation of Group "A" employees	Full powers in respect of all Group "A" officers except in case of Professor and Additional Professor	Full powers in case of Director, Professor and Additional Professor	-		In the case of Director subject to ratification by the Institute

23.	Power to permit the officers of the Institute while going abroad for attending meeting, conference, seminar, workshop, symposia or for short assignments	Full powers except in the case of Director on the basis of leave of the kind due and admissible upto the period of thirty days, and that the faculty members concerned receives proper invitations from the sponsors of the meeting	Full powers beyond a period of 30 daysinthe case of employees and full powers in respect of Director	-		Subject to directions issued by the Central Government from time to time
24.	Power for treating the absence as on duty for participation in the International scientific conferences/symposia/seminars/ abroad by the members of the Faculty	Full powers up to a maximum of fifteen days inclusive of travel	Full powers beyond a period of fifteen days	-		Subject to directions issued by the Central Government from time to time
25.	Power to allow retention of lien in the Institute for employees when they are appointed elsewhere	Full powers for Group C & D posts up to a maximum of two years. One year at a time	Full powers for Group "B" Posts	Full Powers for Group 'A' posts	-	-
26.	Power for fixation of pay of Institute employees under the Rules	Full powers	-	-	-	-
27.	Power to permit the officers of the Institute to go abroad in connection with the work of the Institute and treatment of absence as on duty	Full powers up to thirty days provided there are no financial implications other than the periods spent in connection with the work of the institute being treated as on duty	Full powers beyond a period of thirty days			Subject to directions issued by the Central Government from time to time
28.	Power to accept Research grant if these are for durations not exceeding three years.	Full powers subject to the general policy of Government of India	-	-	-	

29.	Power to accept the terms and conditions on foreign service terms in respect of a deputationist of Central/State Government where the terms are of usual nature	Full powers	-	-	-	-
30.	Power to grant extension of tenure of senior Residents/Tutors.	Full powers	-	-	-	-
31.	Power to grant advance increments on the recommendations of the selection committee	Full power up to three advance increments	Full powers beyond three advance increments	-	-	-
32.	Power to grant advance increment under Fundamental Rules 27 to employees of Research Schemes on their appointment to regular posts in the Institute	Full powers on to the merit of each case	-	-	-	-
33.	Power to relax the provision of Supplementary Rule 12 where the subsistence allowance to be received is in the nature of daily allowance and an honorarium is involved	Full powers	-	-	Subject to the directions issued by the Central Government from time to time	-
34.	To declare an Institute employees to be a ministerial servant	Full powers	-	-	-	-
35.	To suspend a lien	Full powers provided that he is authorised to take appointments to the posts on which the lien is held	Full powers for all other posts	-	-	-
36.	To transfer the lien of an Institute employees from one post to another	Full powers provided that he is authorised to make appointment to both the posts concerned	Full powers for all other posts	-	-	-
37.	To transfer an Institute employee from one post to another	Full powers in the case of Group B, C &D employees	Full powers in case of group B employees	Full powers in case of group A employees	-	-

38.	Fixation of pay and allowances of an Institute employees treated as on duty under Fundamental Rule (9) (6) (b)	Full powers in the case of B, C& D employees	Full powers in case of Group 'A' employees	-	-	-
39.	Counting extraordinary leave for increments.	Full powers in the case of Group B, C & Demployees	Full powers in the case of Group 'A' employees	-	-	-
40.	Power to reduce the pay of an officiating Governing Servant	Full powers in the case of Group B, C and D employees	Full powers in the case of Group'A' employees			
41.	To sanction grant of and to permit acceptance of honorarium	Full powers up to a maximum of Rs. 5000/- per annum in each case in accordance with the .provisions of rule 46 (B) of Fundamental Rules and Government of India's order issued there under from time to time for all categories of employees. In the case of recurring honoraria this limit applies to the total of recurring payments make to an individual in a year. In case of Group A & Group B employees the matter shall be reported to the Governing Body.	-	-	-	-
42.	Power to appoint an employee to hold temporarily to officiate in more than one post and to fix the pay of subsidiary posts and the amount of compensatory allowance to be drawn.	Full powers subject to rules applicable to similar classes of Central Government Employees.	-	-	-	-

43.	To declare the grade of fee paid to part time employees (for purpose of Travelling Allowances)	Full powers				
44.	To decide the shortest or cheapest of two or more routes.	Full powers				
45.	To allow mileage allowances by a route other than the shortest or cheapest	Full powers provided selection of the route is in Institutes interest.				
46.	To decide the point of commencement or end of journey in a station	Full powers				
47.	To declare that an Institute employee whose pay does not exceed Rs.300/- per mensem is entitled to lowest class accommodation in a steamer	Full powers	-	-	-	-
48.	To declare in case of doubt on hardship the class of steamer accommodation to which an Institute employees is entitled	Full powers				
49.	Power to require a medical certificate of fitness before return from leave.	Full powers	Full powers in the case of Director			
50.	Extension of leave to cover over-stay	Full powers provided that the employee on leave will on return be under the administrative control of the Institute	Full powers in all other cases	-	-	-
51.	To sanction transfer to foreign service in India and to fix the pay in foreign service	Full Powers in respect of Group B, C, and D employees, subject to the conditions mentioned in column 5 against Serial No. 30 in appendix 4 of the post & Telegraph compilation of fundamental and	Full powers in respect of Group A employees	-	-	-

		supplementary Rules, Vol.II				
52.	To decide the date of reversion of Government servant who takes leave before reversion from foreign service	Full Powers	-	-	-	-
53.	Power to sanction the undertaking of work for which a fee is offered and the acceptance of a fee	Full powers	-	-	-	-
54.	Travel by Air by Officerin relaxation of rules	Full powers in case of Urgency and necessity	-	-	-	-
55.	To declare that pay of an Institute employee includes compensation for all journey by road.	Full powers in the case of Group B, C and D employees	Full powers in case of Group A employees			
56.	Power to grant exemption from the rule limiting a halt on tour to ten days.	Full powers up to a limit of 30 days	Full powers beyond a period of 30 days	-	-	-
57.	Power to fix amount of hire or charges where an Institute employee is provided with means of locomotion at the expense of the Institute etc. but pays all the costs of its use of propulsion	Full powers				
58.	To grant travelling allowance to non-officials attending commission of enquiry etc. and to fix their grade.	Full powers	-	-	-	-
59.	To declare who shall be controlling officer and to make rules for his guidance	Full powers , provided an Institute employee is not declared his own controlling officer	-	-	-	-
60.	To grant leave other than special disability leave	Full powers				
61.	To grant leave when a medical board has reported that there is no reasonable prospect of the employee being fit to return to duty.	Full powers	-	-	-	-

62.	To decide in case of doubt whether a particular employee is serving in a vacation Department	Full powers	-	-	-	-
63.	To grant maternity, and hospital leave.	Full powers	-	-	-	
64.	Topermit calculation of joining time by a route other than that which travellers ordinarily use.	Full powers	-	-	-	-
65.	To extend joining time within a maximum period of thirty days	Full powers	Full powers beyond thirty days	-	-	-
66.	Authorising an Institute employee to proceed on duty to any part of India.	Full powers in case of Group B, C and D employees	Full powers in case of Group A employees	-	-	-
67.	Power to alter in the case of clerical errors in the date of birth recorded in the service rolls of Institute employees	Full powers in case of Group 'C' & 'D' employees	Full power in the case of Group 'A' and 'B' employees	-	-	-
68.	Power to sanction investigation of claims for arrears of pay etc. which are more than three years but not more than six years old.	Full powers	Full powers in other cases.	-	-	-
69.	Power to sanction permanent advances in respect of employees other than Director	Full power	Full power in the case of Director	-	-	-
70.	Power to issue instructions to subordinate authorities in the matter of contingent expenditure.	Full powers	-	-	-	-
71.	Disposal of obsolete surplus and unserviceable stores	Full powers	-	-	The Director shall Act on the advice of condemnation Board set up for the purpose by the Institute	
72.	Power to vary the terms of repaying of advances granted to Institute employees in exceptional cases	Full powers in cases in which he is competent to sanction the grant of advances	To all other cases	-	-	-

		provided that in the case of interest bearing advances, the period of repayment not extended.				
73.	Power to sanction advances for purchase of conveyance	Full power in the cases of Institute employees holding permanent posts, subject to the limits and conditions laid down in Rules 199 to 218 of General Finance Rules.	-	-	-	-
74.	Power to authorise the sale or transfer of motor vehicles purchased with advance from the institute.	Full powers in cases mentioned in clauses (V) of Rule - 256 of General Finance Rule.	-	-	-	-
75.	Power to extend up to a maximum of 24 the number of instalments in which an advances granted for the purchase of a bicycle should be repaid to the Institute.	Full powers				
76.	Power to sanction advances to Institute employees on tour, transfer	Full power in case of Institute employees, holding permanent or temporary posts subject to the limits and conditions laid down in Rule 231 to 234 of General Finance Rules	-	-	-	-
77.	Power to sanction advances for the lawsuit to which Institute is a party.	Full power	--	-	-	-
78.	Power to prescribe the term of security bond to be executed by a subordinate authority, entrusted with the custody of cash, storms.	Full powers	-	-	-	-

79.	Power to sanction advances of pay on the eve of important festivals. Under the Treasury Rules	Full powers	-	-	-	-
80.	Power to authorise a departure from the provisions of the Rules 109 (1) relating to custody of Institute money.	Full power		-	-	-

SCHEDULE II

(See regulation 33)

The Appointing, Disciplinary and Appellate Authority for the various posts in the Institute

Sl. No.	Description of Posts	Appointing Authority	Authority competent to impose penalty or penalties which it may impose with reference to Rule - 11 of the Central Civil Services (Classification Control and Appeal) Rules, 1965		Appellate Authority
			Disciplinary Authority	Penalties under Rule- 11 of the Central Civil Services (Classification, Control and Appeal) Rules, 1965.	
1	2	3	4	5	6
1	Group 'A' Posts (i) Director	Institute subject to Rule - 7 of the All India Institute of Medical Sciences Rules.	Institute	All, subject to condition that penalties (v) to (ix) shall not be imposed without the prior approval of the Central Government	
	(ii) Other Posts	Governing Body	(a) Governing Body (b) President	(a) All Penalties (b) Penalties (i) to (iv)	(a) Institute Governing Body
2	Group 'B' posts	President	(c) President (d) Director	(c) All Penalties (d) Penalties (i) to (iv)	(b) Governing Body (c) President
3	Group 'C' posts	Director	(a) Director	(a) All penalties	(a) President
4	Group 'D' posts	Director	(a) Director (b) Deputy Director (Administration) in the case of Institute employees other than those provided in (c) and (d) below (c) Medical Super intendent in the case of All India Institute of Medical	(a) All Penalties (b) Penalties (i) to (iv) (c) Penalties (i) to (iv) (d) Penalties (i) to (iv)	(a) President (b) Director (c) Director (d) Director

			Sciences Hospital employees. (d) Chief Organiser, Dr.Rajendra Prasad Centre for Ophthalmic Sciences and Chiefs of other Centres as and when established by the Institute in the case of the employees working in the Centres concerned.		

(i) Authorisation of the Director, All India Institute of Medical Sciences to issue the Charge-sheet and statement of allegation, penalties and suspension orders after obtaining the approval of the Governing Body, the President, All India Institute of Medical Sciences, as the case may be. The notice, the charge-sheet and statement of allegations shall be signed by the Director for and on behalf of the Governing Body or the President, as the case may be, and the documents shall also expressly state this fact. Phrases like "By order of the Governing Body" or "the President" or the "approval by the Governing Body" or the "President" can be used on such documents.

(ii) Since the Governing Body meeting are fixed at intervals, the Chairman of the Governing Body is authorised to initiate disciplinary proceedings against employees of Group A and faculty members and the final decision on penalty shall be taken in the Governing Body meeting.

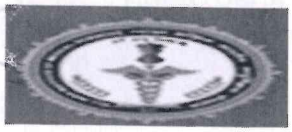
By the Authority of the Institute

RANDEEP GULERIA, Director

[ADVT.-III/4/Exty./248/19]

Uploaded by Dte. of Printing at Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.

ALOK KUMAR Digitally signed by ALOK KUMAR Date: 2019.10.23 13:44:45 +05'30'



Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Comprehensive Cyber Security Audit Policy Guidelines reg-

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Wed, Dec 17, 2025 at 3:15 PM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **mn mishra** <mnmishra.mohfw@gmail.com>
Date: Tue, Aug 12, 2025 at 12:50 PM
Subject: Fwd: Comprehensive Cyber Security Audit Policy Guidelines reg-
To: <dda@aiimsdeoghar.edu.in>, DDA AIIMS Jodhpur <dda@aiimsjodhpur.edu.in>, DDA AIIMS Bhopal <dydir@aiimsbhopal.edu.in>, <ddamadurai1189@gmail.com>, Deputy Director Administration <dda@aiimsbhubaneswar.edu.in>, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Rishikesh <dda@aiimsrishikesh.edu.in>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, <ddaaiimsjammu@gmail.com>, ddaaiimsbilaspur <ddaaiimsbilaspur@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, <dda@aiimsnagpur.edu.in>, Dy Director Administration AIIMS, Raebareli <ddaaiimsrbl@gmail.com>, Recruitment Cell AIIMS, Bathinda <recruitmentaiimsbathinda@gmail.com>, <ciso@aiimsraipur.edu.in>, <ciso@aiimskalyani.edu.in>, <anandchellappan@aiimsnaqour.edu.in>, <shivam.tsg@aiimsbhopal.edu.in>, <head.it@aiimsjammu.edu.in>, <rohit.bio@aiimsbibinagar.edu.in>, <drraje.path@aiimsmadurai.edu.in>, <drmohanraj@aiimsgorakhpur.edu.in>, <drabhyuday@aiimspatna.edu.in>, <raj.sharma@aiimsbhubaneswar.edu.in>, <Goyal.tarun@aiimsbathinda.edu.in>, AIIMS Gorakhpur <itcellaiimsgkp@gmail.com>, <draksharphc@gmail.com>, <itincharge@aiimsrishikesh.edu.in>, <aao@aiimsdeoghar.edu.in>, <mundraa@aiimsjodhpur.edu.in>, <debboruah@aiimsguwahati.ac.in>
Cc: RaviKumar RaviKumar <ravi.kumar89@gov.in>, dharmenderkumar14 <dharmender.kumar14@gov.in>, ShriRajKumar Under Secretary <raj.kumar28@nic.in>, <arvind.thakur@nic.in>, <shalaka.kujur@nic.in>, <abhijit.69@gov.in>, ANKITA MISHRA BUNDELA <js-pmssy-mohfw@gov.in>

Sir/Madam,

Kindly refer to the attached MeitY Office Memorandum dated **29 July 2025** and the *Comprehensive Cyber Security Audit Policy Guidelines, Version 1.0, dated 25 July 2025*, regarding the subject cited above.

This is forwarded for your kind information and necessary action, please.

Encl.: As above

--
regards,
Er.M.N.Mishra,
PMSSY,MoHFW,
Mob: 7982125857
---------- Forwarded message ---------
From: **Shri Raj Kumar Deputy Secretary** <raj.kumar28@nic.in>
Date: Tue, Aug 12, 2025 at 12:32 PM
Subject: Fwd: Comprehensive Cyber Security Audit Policy Guidelines reg-

To: Dharmendra Kumar <dharmender.kumar14@gov.in>, Ravi Kumar <ravi.kumar89@gov.in>, SUBHANSHU KUMAR <subhanshu.kumar@gov.in>, mnmishra.mohfw <mnmishra.mohfw@gmail.com>

Deputy Secretary
PMSSY-I/ SNA
23063178

========== Forwarded message ==========
From: ANKITA MISHRA BUNDELA <js-pmssy-mohfw@gov.in>
To: "Shri Raj Kumar Deputy Secretary"<raj.kumar28@nic.in>
Date: Tue, 12 Aug 2025 11:54:15 +0530
Subject: Fwd: Comprehensive Cyber Security Audit Policy Guidelines reg-
========== Forwarded message ==========

========== Forwarded message ==========
From: eHealth Section <telmed-mohfw@gov.in>
To: "Jaideep Kumar Mishra"<asfa-mhfw@nic.in>, "Ms. Roli Singh"<ash-mohfw@nic.in>, "Ms VHekali Zhimomi" <zhimomiv@ias.nic.in>, "Aradhana Patnaik"<asmd-mohfw@nic.in>, "Manashvi Kumar"<jstraining-mohfw@gov.in>, "UMESH KUMAR MISRA"<ofc.asme-mohfw@gov.in>, "oo.asphp Singh"<oo.asphp-mohfw@gov.in>, "ELANGBAM ROBERT SINGH"<robert.elangbam@gov.in>, "Indrani Kaushal"<ea-mohfw@gov.in>, "gulam mustafa" <gulam.mustafa@nic.in>, "JS ME"<js.me-mohfw@nic.in>, "ANKITA MISHRA BUNDELA"<js-pmssy-mohfw@gov.in>, "Nikhil Gajraj"<nikhil.g@ias.nic.in>, "Vijay Nehra"<js-proc-mohfw@gov.in>, "Saurabh Jain"<js.policy-mohfw@gov.in>, "Vandana Jain"<vandana.jain@nic.in>, "Meera Srivastava"<jsrch-mohfw@gov.in>, "Vijay Sinha" <sinha.vijay@nic.in>, "Indrani Kaushal"<ea-mohfw@nic.in>, "Pradeep Khasnobis"<pradeep.khasnobis@gov.in>, "Rakesh Kumar Maurya"<rakesh.maurya@gov.in>, "Narendra Oza"<nk.oza@gov.in>, "KIRAN KARLAPU" <kiran.karlapu@gov.in>, "Harsh Mangla"<harsh.mangla@ias.nic.in>, "SAROJ KUMAR"<saroj.kumar@nic.in>, "Sachin Kumar"<sachin.k@nic.in>, "SUSHIL Gahlaut"<sp.gahlaut@nic.in>, "Kumar Rahul"<kumar.rahul@nic.in>, "Gs Chitra"<gs.chitra@nic.in>, "Phool Prasad"<prasad-upsc@gov.in>, "Govind Kumar"<govind.bansal78@gov.in>, "PRIYADARSHIKA SRIVASTAVA"<priyadarshika.s@gov.in>, "Anjana Rajkumar"<director-cghs@cghs.nic.in>, "R.K. Singh"<rk.singh27@nic.in>, "Indranil Das"<indranil.das@gov.in>, "Dinesh Kumar"<dinesh.kumar14@nic.in>, "Nikhil Agarwal"<nikhilkr.agarwal@nic.in>, "Poonam Meena"<poonam.22@gov.in>, "Mrs Bharti Sahai" <bharti.sahai@nic.in>, "Noorin Bux Khan"<noorinbux@ord.gov.in>, "ghalmevc"<ghalme.vc@gov.in>, "naveenaggarwal"<naveen.aggarwal@ias.gov.in>, "Bherav Dutt"<bherav.dutt@nic.in>, "Samsul Haque" <samsul.haque@nic.in>, "DR.PULKESH KUMAR"<dr.pulkesh@gov.in>, "Z. A. Khan"<us-doj@mha.gov.in>, "Manoj Kumar Sinha"<mk.sinha26@nic.in>, "Sarvajit Kumar"<kumar.sarvajit@nic.in>, "G A Raghuvanshi"<gopal.aaditya@nic.in>, "Sarita Nair"<sarita.nair@gov.in>, "Rajesh Kumar verma"<rajeshkumar.verma@nic.in>, "KAMAL ARORA DS"<kamal.arora@nic.in>, "abhijit cgca"<abhijit.cgca@gov.in>, "KAUSTUBH GIRI"<dsnhmfin-mohfw@gov.in>, "NAVEEN AGGARWAL"<naveen.aggarwal@ias.nic.in>, "Aashima Bhatnagar"<aashima.bhatnagar@gov.in>, "Arvind Thakur"<arvind.thakur@nic.in>, "RAJENDRA PRASAD SATI DEPUTY SECRETARY"<rp.sati88@nic.in>, "vivekgupta"<vivekgupta@aiims.gov.in>, "MEDICAL SUPERINTENDENT"<msoffice@vmmc-sjh.nic.in>, "spsood" <spsood@cdac.in>, "Achyut Patil"<achyutp@cdac.in>, "'gaurs'"<gaurs@cdac.in>, "rsp"<rsp@nihfw.org>, "gaurav sharma"<gaurav.sharma@nihfw.org>, "med rmlh"<med.sup.rmlh@gmail.com>, "director"<director@aiimsbhopal.edu.in>, "director"<director@aiimsbhubaneswar.edu.in>, "director"<director@aiimsjodhpur.edu.in>, "director"<director@aiimspatna.org>, "director"<director@aiimsraipur.edu.in>, "director"<director@aiimsrishikesh.edu.in>, "director"<director@aiimsmangalagiri.edu.in>, "directoraiimsnagpur"<director aiimsnagpur@gmail.com>, "drppjoshi"<drppjoshi@aiimsnagpur.edu.in>, "Edaiimsrbl"<edaiimsrbl@gmail.com>, "executivedirector"<executivedirector@aiimsgorakhpur.edu.in>, "Ed"<ed@aiimskalyani.edu.in>, "Director" <director@aiimsdeoghar.edu.in>, "Director Bibinagar"<director@aiimsbibinagar.edu.in>, "Director"<director@aiimsbilaspur.edu.in>, "sharmadn"<sharmadn@aiims.edu>, "shakti810505"<shakti810505@gmail.com>, "director" <director@aiimsjammu.edu.in>, "Drmhraosvims1957"<drmhraosvims1957@gmail.com>, "director"<director@aiimsguwahati.ac.in>, "madhabananda"<madhabananda@gmail.com>, "sachimohanty"<sachimohanty@rediffmail.in>, "sharmadn"<sharmadn@aiims.edu.in>, "Rangoli Pathak"<rv.rangoli@gov.in>
Cc: "Madhukar Bhagat"<jsehealth-mohfw@gov.in>, "REENA SHARMA"<reena.sharma80@gov.in>, "HarishKumarJain PPS"<harish.jain68@gov.in>, "SWARUP DUTTA"<hod-mohfw@nic.gov.in>, "Pawan Kumar" <pawan.kumar13@nic.in>, "Sudidhi Das"<dciso-cstmhfw@nic.gov.in>, "Avinash Yadav" <avinash.yadav73@gov.in>, "ehealthmohfw1"<ehealth.mohfw1@gmail.com>
Date: Mon, 11 Aug 2025 17:56:52 +0530
Subject: Comprehensive Cyber Security Audit Policy Guidelines reg-
========== Forwarded message ==========

Sir/Madam,

Kindly refer to the attached MeitY **OM dated July 29,2025** and Comprehensive Cyber Security Audit Policy Guidelines, version 1.0, dated 25-07-2025 regarding the subject cited above. This is for your kind information and necessary action please.

Regards
eHealth Section
Ministry of Health & Family welfare
Room No.-213, D-wing, Nirman Bhawan
New Delhi-110011
Tel No.-23062263

2 attachments

Cyber security Audit policy.pdf
309K

Comprehensive_Cyber_Security_Audit_Policy_Guidelines_july 2025.pdf
541K

No. 1(1)/2023-Cyber Security
Government of India
Ministry of Electronics and Information Technology

4399416
8/8/25

Electronics Niketan, 6, CGO Complex
Lodhi Road, New Delhi-110003
Dated: July 29, 2025

Office Memorandum

Subject: Comprehensive Cyber Security Audit Policy Guidelines

With the increasing number of cyber threats and the need for robust protection measures in today's digital landscape, cyber security is a major concern for enterprises. The regular cyber security audits and assessments help organizations to strengthen their security posture, identify critical vulnerabilities, and ensure compliance with regulatory requirements.

2. In an effort to promote a seamless, effective, and efficient security auditing process, the Indian Computer Emergency Response Team (CERT-In) has issued "Comprehensive Cyber Security Audit Policy Guidelines". The guidelines are available on website of CERT-In through the following URL:

https://cert-in.org.in/PDF/Comprehensive_Cyber_Security_Audit_Policy_Guidelines.pdf

3. The purpose of these guidelines is to offer thorough guidance for both the auditee and auditing organizations involved in cyber security audits. It serves as a comprehensive guide to facilitate a productive partnership throughout the audit process, fostering mutual responsibility and driving meaningful enhancements in security, risk mitigation, and regulatory adherence to safeguard sensitive information.

4. In view of the above, it is requested that necessary action may please be taken to adhere with the guidelines.

This issues with the approval of Secretary, MeitY.

Savita Utreja
29.7.2025

(Savita Utreja)
Scientist G
Tel: 011-24368146
Email: sutreja@meity.gov.in

To,

Heads of all MeitY organisations:

NIC, STQC, CERT-In, CCA, UIDAI, DIC, NeGD, MyGov, C-DAC, NIELIT, STPI, ERNET, NIXI. NICSI, SAMEER, C-MET, CSC, BISAG-N, SCL

Secy(H) - in meeting
JS(eHealth)

PI available on priority
DIR (eHealth)

सत्यमेव जयते

Comprehensive Cyber Security Audit Policy Guidelines

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India

Version 1.0 | 25.07.2025

Table of Contents

1. Introduction 3
2. Authority for Issuance of Guidelines 4
3. Objective of the Document 6
4. Applicability 7
5. Definitions 8
6. Scope of Engagements Covered 14
7. Basic principles in Audit 19
8. Applicable standards and Frameworks 22
9. Auditee Responsibility 25
10. Auditor Responsibility 30
11. Quality control of auditing organisations involved in Audit 36
12. Selection of Auditor 37
13. Planning the Audit 41
14. Agreeing on the Terms of Engagement and Revisions to the Scope 51
15. Performance of the Audit 53
16. Forming an Opinion, Conclusion and Reporting 58
17. Communication with those Charged with IT Governance 62
18. Audit Evidence and Documentation 64
19. Consequences of Non-Compliance to Guidelines and Terms and Conditions of Empanelment 66
20. Conclusion and Feedback mechanism 69

1. Introduction

Given the increasing number of cyber threats and the need for strong protection measures in today's digital landscape, cyber security is a major concern for enterprises. An organization's security posture can be improved, vulnerabilities detected, and regulatory compliance ensured with the help of regular cyber security audits and assessments. In an effort to promote a seamless, effective, and efficient auditing process, this document offers thorough guidance for both the auditee and auditing organizations involved in cyber security audits.

These guidelines serve two purposes. Firstly, they assist organizations being audited (auditees) in preparing for audits, understanding requirements, and addressing deficiencies. This helps ensure that their cyber security measures align with industry standards and regulations, enabling proactive improvement of security practices.

Secondly, the guidelines provide auditing organizations with a structured framework to conduct rigorous, fair, and transparent cyber security audits. They outline the auditor's responsibilities, methodologies, and best practices, enabling them to provide independent, impartial and constructive recommendations that strengthen the auditee's cyber security.

The success of a cyber security audit relies on the collaborative efforts of both the organization being audited and the auditing entity. This document serves as a comprehensive guide to facilitate a productive partnership throughout the audit process, fostering mutual responsibility and driving meaningful enhancements in security, risk mitigation, and regulatory adherence to safeguard sensitive information.

2. Authority for Issuance of Guidelines

Whereas, sub-section (1) of section 70B of the Information Technology (IT) Act, 2000 (21 of 2000) provides that the Central Government shall appoint an agency of the Government to be called the Indian Computer Emergency Response Team and the Central Government *vide* notification dated the 27th October, 2009, has appointed the Indian Computer Emergency Response Team as the agency for the purposes of the said Act, which is now referred as CERT-In or ICERT.

And whereas, sub-section (4) of section 70B of the said Act provides that the Indian Computer Emergency Response Team shall perform prescribed functions in the area of cyber security: -

a) collection, analysis and dissemination of information on cyber incidents;
b) forecast and alerts of cyber security incidents;
c) emergency measures for handling cyber security incidents;
d) coordination of cyber incidents response activities;
e) issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
f) such other functions relating to cyber security as may be prescribed.

And whereas, the provisions of sub-section (5) of the section 70B of IT Act, 2000 provides that the manner of performing functions and duties of the agency referred to in sub-section (1) shall be such as prescribed and Central Government has notified Information Technology (The Indian Computer Emergency Response Team and Manner of performing functions & duties) Rules, 2013 to this effect. The provision of rule no.9 of

these Rules, 2013, inter-alia, prescribes the activity of Information security assurance and audit to CERT-In.

And whereas, as per provisions of sub-section (6) of section 70B of the IT Act, 2000, CERT-In is empowered and competent to call for information and give directions to the service providers, intermediaries, data centres, body corporate and any other person to carry out the activities enshrined in sub-section (4) of section 70B of the IT Act, 2000. The failure to provide the information or non-compliance of the direction issued under sub-section (6) attract punitive action in terms of provisions of sub-section (7) of section 70B of the IT Act.

Now, therefore, these guidelines are herein issued by CERT-In in discharge of its statutory authority and responsibility to enhance the cyber security posture of the nation, which are binding on all CERT-In empanelled auditing organizations and auditee entities covered under the relevant provisions.

3. Objective of the Document

The primary objective of this Comprehensive Cyber Security Audit Policy Guidelines document is to provide a structured and standardized framework for conducting cyber security audits within organizations. The guidelines are intended to serve as a reference for both CERT-In empaneled auditing organizations and auditee organizations to ensure that cyber security audits are carried out in a consistent, effective, and secure manner.

The document outlines the processes, methodologies, and best practices required for conducting thorough and accurate assessments of an organization's cyber security posture. It aims to:

i. Establish Uniform Standards: Ensure that all cyber security audits follow a common set of standards and procedures, thereby promoting consistency in audit quality, evaluation criteria, and reporting.
ii. Provide Clarity for Auditors and Auditees: Define the roles, responsibilities, and expectations for both auditing organizations and auditee organizations, ensuring mutual understanding of the audit process and deliverables.
iii. Promote Continuous Improvement: Encourage auditee organizations to continuously improve their cyber security measures by identifying weaknesses and implementing corrective actions, leading to enhanced overall security posture.

This document will act as a comprehensive guide for the audit process, from initial planning through to final reporting and follow-up actions, contributing to the overarching goal of safeguarding the nation's cyber infrastructure from threats.

4. Applicability

This guideline has been issued by Indian Computer Emergency Response Team (CERT-In) and is applicable to the following entities:

i. **CERT-In empaneled Auditing Organizations:** Indian Computer Emergency Response Team (CERT-In) empanels Information Security Auditing Organizations to undertake audits, including vulnerability assessments and penetration testing of computer systems, networks and applications of various organizations of the Government and of other sectors of the country. The empaneled auditing organizations agree to provide cyber security auditing services in accordance with the commercial contract to be entered into with the auditee organizations and abide by all the conditions of empanelment as well as service delivery.

ii. **Auditee Organizations:** It is the organization that owns or operates the systems, processes, and infrastructure that is being evaluated or assessed by the CERT-In empaneled auditing organisations. These guidelines are intended for organizations in both the public and private sectors that are required to or are seeking to evaluate their cyber security posture, identify vulnerabilities, assess risks, and ensure compliance with applicable regulatory standards and industry best practices.

5. Definitions

i. **Cyber Security Audit** - A systematic and independent assessment of an organization's security controls, policies, and procedures to evaluate their effectiveness in protecting information systems and data from cyber threats.

ii. **Scope of Audit** – The defined parameters of an audit engagement, specifying the systems, functions, departments, assets, and processes to be evaluated.

iii. **Audit Evidence** – Any information, documentation, logs, observations, or other forms of data collected during the audit that substantiate audit findings and support conclusions. Audit evidence must be accurate, relevant, and sufficient to validate the audit's objectives and must be properly documented and appended to the audit report.

iv. **Working Notes** – Internal documentation created and maintained by auditors during the audit process, capturing audit activities, methodologies employed, evidence gathered, and preliminary findings. These notes serve as a record to substantiate conclusions and facilitate subsequent review and verification. The Auditing organization to ensure adherence to "Policy Guidelines for Handling Audit related Data" published on CERT-In's website (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/Policy_Guidelines_Handling.pdf)

v. **Observation** – A documented finding resulting from the audit process, identifying either conformity or deviations from established controls, standards, or procedures. Observations are supported by objective, verifiable evidence and may indicate potential areas of improvement or non-compliance.

vi. **Non-Conformity / Non-Compliance** – A condition wherein a process, control, or practice fails to meet the prescribed standards, regulatory requirements, or internal policies. Non-conformities may indicate gaps or weaknesses in the control environment that require corrective action.

vii. **Root Cause Analysis (RCA)** – A systematic investigative process used to identify the fundamental causes or underlying factors that contribute to an incident, audit finding, or failure. RCA seeks to address the source of the issue rather than merely its symptoms to ensure effective corrective actions.

viii. **Closure Report** – A comprehensive report generated at the conclusion of the audit, indicating that all audit observations, findings, and issues have been addressed, remediated, or closed. The closure report confirms that the audit engagement has met its objectives and that all necessary corrective actions have been taken.

ix. **Threat** – A potential event or condition that could exploit a vulnerability and result in harm, disruption, or damage to a system, organization, or its assets. Threats may be natural, technological, or human in nature.

x. **Risk** – The probability and impact of a threat exploiting a vulnerability, often quantified as the likelihood of occurrence and the severity of potential consequences. Risk assessment typically involves evaluating the combination of threat likelihood and the magnitude of impact to determine the risk level.

xi. **Security Posture** – The overall security standing of an organization's information systems, networks, and associated controls at a specific point in time. This posture reflects the organization's ability to prevent, detect, and respond to security incidents effectively.

xii. **Control or Security Control** – A measure, safeguard, or countermeasure implemented to mitigate risk, enforce security policies, and protect the confidentiality, integrity, and availability of systems, data, and assets. Controls may be administrative, technical, or physical in nature, and are designed to reduce vulnerabilities and prevent threats from exploiting them.

xiii. **Network Infrastructure** – The collection of physical and virtual components, including but not limited to routers, switches, firewalls, communication cables, and associated software, that enable data transmission and ensure the security and reliability of network operations within an organization.

xiv. **Staging Environment** – A non-production, controlled environment that replicates the production environment, where applications, software, or system configurations are thoroughly tested and validated prior to deployment in the live, operational environment.

xv. **Production Environment** – The live, operational setting where the organization's systems, applications, and services are actively used by end-users.

xvi. **Non-Disclosure Agreement (NDA)** – A legally binding contract between parties, obligating confidentiality regarding sensitive or proprietary information exchanged during the audit engagement. The NDA ensures that audit-related data, findings, and communications remain confidential and are not disclosed without proper authorization.

xvii. **Conflict of Interest** – A situation in which an auditor's personal, financial, or organizational interests may influence or compromise their ability to conduct the audit in an objective and impartial manner. Such conflicts must be disclosed and managed to maintain the integrity and credibility of

the audit process. This includes scenarios where the same entity is involved in both the implementation of controls and their subsequent audit, or in conducting audits while also being responsible for remediation activities. Such overlaps create inherent conflicts that undermine the independence of the audit process. All such conflicts must be disclosed and managed to maintain the integrity and credibility of the audit process.

xviii. **Common Vulnerabilities and Exposures (CVE)** – A publicly disclosed, standardized list of unique identifiers assigned to known cyber security vulnerabilities. Each CVE entry contains a distinct identifier, a brief description of the vulnerability, and references to additional resources. CVE serves as a common language for tracking and sharing information about vulnerabilities across various platforms and organizations.

xix. **Common Weakness Enumeration (CWE)** – A community-developed, list of common software and hardware weaknesses that may lead to security vulnerabilities. A "weakness" refers to an inherent flaw or condition within software, firmware, hardware, or services that, under specific conditions, may introduce risks or vulnerabilities.

xx. **Denial of Service (DoS) & Distributed Denial of Service (DDoS) Testing** – A simulated attack on a system designed to assess its capacity to withstand traffic overloads or service disruptions. DoS and DDoS testing measure the resilience of systems to prevent downtime and maintain service availability during high-volume and malicious traffic events.

xxi. **Vulnerability Assessments**- Examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of

proposed security measures, and confirm the adequacy of such measures after implementation.

xxii. **Penetration Testing**- A security testing methodology in which individual components or the application as a whole are actively tested to identify and exploit potential vulnerabilities. The objective is to determine whether these vulnerabilities can be exploited to compromise the application, access sensitive data, or affect the underlying infrastructure and environment.

xxiii. **Red Team Assessment**- An exercise, reflecting real-world conditions, that is conducted as a simulated attempt by an adversary to attack or exploit vulnerabilities in an enterprise's information systems.

xxiv. **Classification of vulnerabilities based on Severity:** In cybersecurity audits and vulnerability assessments, it is crucial to classify vulnerabilities based on their severity to determine appropriate remediation priorities. Two widely adopted frameworks for assessing and classifying severity are:

- CVSS: The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes. It provides a score from 0.0 to 10.0, helping stakeholders understand the risk level and prioritize remediation.
- EPSS: The Exploit Prediction Scoring System (EPSS) is a data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild. The EPSS model produces a

probability score between 0 and 1 (0 and 100%). The higher the score, the greater the probability that a vulnerability will be exploited.

Auditors are required to implement both CVSS and Exploit Prediction Scoring System (EPSS) frameworks within their audit reports. The observations/vulnerabilities in the report must be categorized based on the Common Vulnerability Scoring System (CVSS) for severity and supplemented with the Exploit Prediction Scoring System (EPSS) to assess the likelihood of real-world exploitation.

6. Scope of Engagements Covered

The types of cyber security audits and assessments including, but not limited to, those listed below, may be carried out and fall within the scope of this document. Auditee organizations, which are expected to ensure a comprehensive audit covering all aspects of their Information and Communication Technology (ICT) systems at least once a year, may also opt for additional assessments and audits during the year.

i. Compliance Audits- Evaluation of an organization's security practices to ensure they adhere to relevant industry standards, regulations, and policies.

ii. Risk Assessments- The process of identifying and evaluating risks arising from cyber threats, vulnerabilities, and potential cyberattacks that could impact organizational operations, organizational assets, individuals, and connected entities. This involves assessing the likelihood and impact of various cybersecurity incidents.

iii. Vulnerability Assessments- Examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

iv. Penetration Testing- A security testing methodology in which individual components or the application as a whole are actively tested to identify and exploit potential vulnerabilities. The objective is to determine whether these vulnerabilities can be exploited to compromise the application, access sensitive data, or affect the underlying infrastructure and environment.

v. Network infrastructure Audits- Comprehensive review of network components, including hardware devices such as firewall, end point

devices, servers, router, network switches, IPS / IDS etc., software, configurations, access controls, and security measures, to identify vulnerabilities, inefficiencies, and areas for improvement.

vi. Operational Audits- Evaluation of an organization's cyber security operations, processes, and controls to assess their efficiency, effectiveness, and alignment with security objectives.

vii. IT security policy review and assessment against security best practices.

viii. Information Security Testing- The process of validating the effective implementation of security controls for information systems and networks, based on the organization's security requirements.

ix. Source Code Review- Examining an application's source code to identify security vulnerabilities, coding errors, and inefficiencies, ensuring adherence to best practices, coding standards, and regulatory requirements to improve code quality and security.

x. Process Security Testing- Evaluating the security measures and controls within an organization's operational processes to identify vulnerabilities and ensure that sensitive information, systems, and applications are protected from security threats.

xi. Communications Security Testing- Evaluating the security measures implemented on communication channels to identify vulnerabilities and ensure that information transmitted over those channels is protected from unauthorized access, interception, modification, or disruption

xii. Application security testing (including web applications, mobile applications and APIs)- Assessing an application's architecture, components, and configuration to identify security vulnerabilities.

xiii. Mobile Application Security Auditing – A structured evaluation of mobile apps to identify security vulnerabilities, assess data protection, and ensure

compliance with secure development practices.

xiv. Wireless Security Testing- Evaluating the security measures of a wireless network by simulating attacks to identify potential vulnerabilities and ensure the network is protected against unauthorized access and data breaches

xv. Physical Security Testing- assessing and evaluating the physical security measures that protect an organization's assets, including its facilities, equipment, and personnel, from unauthorized access, theft, damage, or other physical threats.

xvi. Red Team Assessment- An exercise, reflecting real-world conditions, that is conducted as a simulated attempt by an adversary to attack or exploit vulnerabilities in an enterprise's information systems.

xvii. Digital Forensic Readiness Assessment- Evaluating an organization's preparedness to effectively collect, preserve, and analyze digital evidence in the event of a security incident.

xviii. Cloud Security Testing- Evaluating and assessing the security measures, configurations, and vulnerabilities of cloud-based systems, applications, and infrastructures

xix. Industrial Control Systems/ Operational Technology Security Testing- Evaluating the cyber security posture of industrial control systems (ICS) and operational technology (OT) networks, specifically designed to identify vulnerabilities and potential threats that could disrupt critical industrial processes, impacting safety, production, and overall system availability within a facility.

xx. Internet of Things (IOT)/ Industrial Internet of Things Security Testing (IIOT)-Evaluating and validating the security posture of connected devices within an IoT network, particularly in industrial settings, by identifying vulnerabilities and potential attack vectors.

xxi. Log Management and Maintenance Audit-Assessing the effectiveness and completeness of system and security log generation, retention, integrity, and monitoring practices, ensuring that logs are maintained in accordance with organizational policies and regulatory requirements to support detection, investigation, and response activities.

xxii. Endpoint Security Assessment-Evaluating the security posture of endpoint devices (e.g., desktops, laptops, mobile devices) by assessing configurations, patching, malware protection, encryption, access controls, and monitoring mechanisms to ensure robust protection against endpoint-based threats.

xxiii. Artificial Intelligence (AI) System Audits – Evaluation of AI systems for security, ethical alignment, transparency, data integrity, and resilience to adversarial manipulation.

xxiv. Vendor Risk Management Audits – Assessment of third-party and vendor cybersecurity practices to identify supply chain risks and ensure alignment with organizational security policies.

xxv. Blockchain Security Audit – A structured assessment of blockchain systems, including smart contracts and infrastructure, to identify vulnerabilities, verify cryptographic integrity, evaluate access controls and consensus mechanisms, and ensure compliance with security best practices and regulatory requirements.

xxvi. SBOM (Software Bill of Materials), QBOM (Quantum Bill of Materials), and AIBOM (Artificial Intelligence Bill of Materials) Auditing – Evaluation of the Software Bill of Materials (SBOM), Quantum Bill of Materials (QBOM), and Artificial Intelligence Bill of Materials (AIBOM) to ensure transparency, traceability, and integrity of components used in software, quantum computing, and AI systems. This audit focuses on identifying known

vulnerabilities, licensing issues, and supply chain risks associated with open-source and third-party components, and verifies adherence to secure development lifecycle practices and regulatory compliance.

7. Basic principles in Audit

The effectiveness of a cyber security audit relies on the adherence to fundamental principles that guide the auditor's conduct, ensuring that the audit process is thorough, unbiased, and meets established standards of quality. The following basic principles serve as the foundation of the audit methodology outlined in this document:

i. **Independence**

Auditors must remain free from bias, conflict of interest, and external influence. Audit findings must be based solely on evidence. To ensure the audit assessment remains objective and free from undue influence, the commercial arrangements between the auditee and the auditing organization must be structured to maintain independence. Especifically, payments to the auditing organization should not be contingent upon the outcome of the audit—whether favorable or unfavorable—nor should they be tied to the submission or approval of any closure reports. Linking payments to audit outcomes or closure status could compromise the impartiality of the assessment and create a conflict of interest. It is recommended that auditing fees be based on predefined scopes, deliverables, and timelines, and not influenced by the findings or the post-audit compliance status of the auditee.

In case the auditing organization faces any pressure tactics, coercion, or undue influence from the auditee that may compromise the independence of the audit, the matter should be promptly escalated to CERT-In for appropriate intervention and resolution.

ii. **Objectivity**

Objectivity refers to the auditor's duty to maintain impartiality and fairness throughout the audit. Auditors must avoid situations that could impair their ability to form unbiased judgments. This includes refraining from accepting gifts, favours, or any other benefits that may influence the audit outcome. The auditor's objective is to present findings and conclusions that are supported by verifiable evidence, without being swayed by external pressures or personal preferences.

iii. **Integrity**

Integrity is fundamental to the audit process. Auditors must act honestly and with strong ethical principles, maintaining a high standard of conduct even in the face of challenges. Integrity also entails a commitment to providing clear, accurate, and truthful reports, reflecting the true state of the auditee's cyber security posture.

iv. **Professional Skepticism**

Auditors should critically assess information, question assumptions, and seek supporting evidence to identify gaps, inaccuracies, or risks not immediately visible.

v. **Professional Judgment**

Informed decisions must be made using experience, evidence, and contextual understanding of the auditee's environment, risk profile, and regulatory requirements.

vi. **Professional Care**

Audits should be performed with diligence, competence, and attention to detail. Auditors must stay updated with evolving threats and follow relevant standards and best practices. Auditors must ensure that their work is

conducted in a manner that meets or exceeds the professional standards required for the engagement.

vii. **Confidentiality**

Throughout the audit process, auditors must protect the privacy and integrity of the information to which they have access, ensuring it is not disclosed without proper authorization. The Auditing organization to ensure adherence to "Policy Guidelines for Handling Audit related Data" published on CERT-In's website (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/Policy_Guidelines_Handling.pdf)

viii. **Transparency and Accountability**

Audit processes, methods, and conclusions should be clearly documented and communicated. Auditors are responsible for ensuring the credibility and reliability of their work.

By adhering to these basic principles, auditors ensure that cyber security audits are conducted with the highest standards of professionalism, rigor, and impartiality without any pressure from the auditee organizations and other stakeholders. These principles not only enhance the credibility of the audit process but also help build trust between the auditing organization, the auditee, and other stakeholders.

8. Applicable standards and Frameworks

i. Auditing organization must utilize industry standard methodologies, best practices for security testing. Solely tools-based testing should be discouraged as tool-based audits may focus primarily on automated processes and may overlook non-automated or manual components of the IT infrastructure. This limitation can result in an incomplete view of the overall security.

ii. The limited lists such as OWASP Top 10, SANS Top 25 and similar, should not be considered as standards or references for audits. Instead, audits should include discovery of all known vulnerabilities based on the comprehensive standards/frameworks like ISO/IEC, Cyber Security Audit Baseline Requirements, CSA Cloud Controls Matrix (CCM) for Cloud Security, Open Source Security Testing Methodology Manual (OSSTMM3), OWASP Web Security Testing Guide for web application security testing, OWASP Application Security Verification Standard (ASVS) for establishing and verifying application security controls, the OWASP Mobile Security Testing Guide (MSTG) for mobile app audits OWASP DevSecOps Maturity Model for assessing Continuous Integration / Continuous Deployment (CI/CD) pipeline security along with applicable regulatory framework and directions & guidelines issued from time to time by agencies such as CERT-In, Government and regulatory bodies.

iii. 'Cyber Security Audit Baseline Requirements' document published on CERT-In's Website (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/CyberSecurityAuditbaseline.pdf) should be used by auditees and auditing organizations to build their audit program.

iv. Guidelines and directions issued by CERT-In and regulators to be included as part of scope of audit by default.

v. **For audits of critical Applications/databases/platform of Ministries, Departments, Secretariats, and Offices, wherever sensitive Personal identifiable information (PII) data is involved, the auditing organization shall verify compliance with the "Comprehensive Audit Program Checklist – Cyber and Information Security Audit" as outlined in the "Guidelines on Mandatory Features of Cybersecurity Architecture to be Ensured in all Ministries/Departments" issued by the Cyber Security Division, Ministry of Electronics and Information Technology. This checklist, comprising 282 control points, shall form the default mandatory audit scope for such entities and must be thoroughly assessed during the audit process.**

vi. Auditing organization must verify the existing policies of the organization against the industry standards and best practices and suggest the necessary improvements, if required.

vii. Auditee organizations must confirm that applications are designed & developed with secure practice prior to commencing any assessment. Organization should incorporate secured application development practices and application owners should ask for adherence to the best practices highlighted in the document "Guidelines for Secure Application Design, Development, Implementation & Operations" published on CERT-In's Website. (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/Application_Security_Guidelines.pdf).

viii. Application developed without any secure design and development practices should not be considered for assessment and audits. The same

should be informed to the auditee organization in writing with a copy marked to CERT-In. Auditee organizations and auditor organizations must confirm that application is designed & developed with secure practice prior to commencing any assessment.

ix. The auditing process should be viewed as a tool for the continual process improvement of the auditee organization's security posture, rather than a mere formality for compliance. Audits must not be conducted solely for the sake of fulfilling regulatory requirements; instead, they should adopt a risk-based and domain-specific approach that aligns with the organization's business context, threat landscape, and operational priorities. The auditor's perspective should be focused on identifying meaningful gaps, refining security processes, and recommending practical, actionable improvements. Further, audit findings and recommendations should be clearly articulated in language that is understandable to executive leadership and decision-makers, enabling informed risk management and strategic decision-making.

9. Auditee Responsibility

9.1 Governance and Oversight by Top Management

i. Top management should review & approve the audit program, scope and remedial measures taken by organization to plug the vulnerabilities highlighted in the audits in a time bound manner.

ii. While cyber security audits are essential for identifying vulnerabilities, assessing risks, and ensuring compliance with security standards, the responsibility for maintaining an efficient and robust cyber security posture ultimately rests with the auditee organization, not the auditor.

iii. The frequency and broad scope of audits should be included in the annual reports. However, these reports should exclude any confidential details, infrastructure or application specifics, vulnerabilities, or related observations.

iv. Auditee organizations should follow cyber security auditing related advisories and directions issued by CERT-In.

9.2 Risk Acceptance and Exception Handling

i. Risk treatment techniques such as retain, avoid, transfer and reduce for any reported vulnerabilities or observations in the application or infrastructure, must be authorized & accepted by the head of the auditee organization.

ii. Any exceptions to reported vulnerabilities or observations in the application must be authorized by the head of the organization, who is the owner of the application.

9.3 Remediation and Follow-up

i. After receiving audit findings, the auditee is responsible for implementing the recommended actions to improve security and mitigate risks.

ii. The auditee organization must act upon the relevant audit findings and strive to improve the IT security.

iii. Vulnerabilities highlighted in audit reports should be patched by owners/developer at the earliest. The responsibility of patching and correction of vulnerabilities is the responsibility of Auditee organization.

iv. Follow-up audits should be included within the scope or RFP proposal and must be conducted by the auditing organization after the closure of vulnerabilities or issues identified during the initial audit.

9.4 Internal Monitoring and Development Practices

i. Continuous internal audits/assessments should be carried out by auditee entities and they are expected to ensure that the necessary competencies and skill sets (including relevant professional experience and qualifications) are available to undertake internal audits/assessments.

ii. Auditee organizations must ensure that 'Secure by Design' principles and secure application development practices are included as mandatory requirements in their RFPs and tenders for application/software development.

9.5 Application Handling and Audit Artifacts

i. The application developer should avoid making any code changes to the audited application or infrastructure, after issuance of the audit certificate. It is recommended that audit-related artifacts, such as

hash values, versions, and timestamps, be captured by the auditee organization and shared with the auditing organization. These details should be prominently featured in the audit certificate and reports.

ii. Version control and change management be effectively implemented so that the assets that were/are part of audit scope can be backtracked.

iii. The audit reports shall be signed only by the manpower declared to CERT-In, as listed in the organization's snapshot information available on the CERT-In website. The report must be signed by the Auditors who conducted the audit. It should then be reviewed and signed by a designated Reviewer who is not part of audit team and is from mid-management, to ensure an unbiased and quality review. Finally, the report must be authorized and signed by the Head of the Auditing Organization (e.g., Director, Partner, or CEO), certifying the completeness, accuracy, and integrity of the audit findings and recommendations. The audit certificate must be signed by both the Lead Auditor and the Head of the Auditing Organization.

9.6 Asset Management and Infrastructure Security

i. The complete audit process of the information infrastructure must be undertaken up by the auditee organization itself, except in cases where there is a specific mandate from a Regulator, Government, or relevant stakeholder. Accordingly, the entire process — from defining the audit scope, selecting the auditing organization, providing access to the information infrastructure, to ensuring closure of all audit observations — must be carried out by the owner of the information infrastructure. This responsibility must not be delegated. However, the organization may seek external support for specialized expertise,

while retaining full ownership and accountability for the security of its information infrastructure.

ii. Organizations should maintain and monitor the inventory of all the authorized assets (both software and hardware). For all the assets, proper patch management mechanism should be in-place to patch the vulnerable software, applications and firmware used by the organization.

iii. Organizations should have secure configuration of assets. Appropriate security measures, such as blocking of unused ports, securing and changing default settings and credentials should be implemented during deployment of equipment and applications.

iv. Organizations need to implement the principle of least privilege across the organization's assets. This means that users, systems, applications, and processes should be granted only the minimum level of access permissions necessary to perform their specific roles or function. This limits the potential impact of security breaches, reduces insider threats.

v. Ensure restricted remote access to the cyber infrastructure. Remote access traffic should be tunneled, encrypted and logged to avoid any misuse. Multi Factor Authentication (MFA) is mandatory for remote access of the cyber infrastructure.

vi. Organizations should only use genuine software in their infrastructure and ensure to update software, application and firmware on regular basis to avoid software vulnerabilities. Organizations should also ensure to use secure protocols over weak vulnerable protocols to avoid vulnerabilities associated with weak protocols.

vii. During onboarding, the auditing organization should deliver a presentation to the auditee organization's Board and senior management, explaining their understanding of the audit scope, the methodology to be adopted, and the associated timelines. Similarly, during the exit conference, the auditing organization should present key findings, highlight the overall security posture, and outline associated risks to support informed decision-making.

10. Auditor Responsibility

10.1 Role and Accountability of the Auditor

i. Auditing serves as an independent assessment of an organization's security practices, systems, and controls. The auditor's role is to evaluate the effectiveness of these measures, verify compliance with relevant standards and regulations, and provide recommendations for improvement. However, the auditor is not responsible for managing or maintaining the organization's security measures directly or indirectly; their responsibility is limited to reviewing and reporting on the state of security at the point in time of the audit.

ii. If any of the assets included in the audit scope are found to be inaccessible during the audit, the auditing organization must promptly inform the auditee and request resolution of the accessibility issues. If the auditee organization is unable to resolve the issues, the affected assets must be explicitly mentioned in the audit report, along with the reasons for their exclusion from the audit and same must be brought to the notice of CERT-In.

10.2 Auditor Personnel: Conduct and Competency

i. During and after the audit assignment, personnel involved must be aware of information classification requirements and adhere to practices that ensure the confidentiality, security, and privacy of information. This includes, but is not limited to, the proper collection, use, disclosure, and protection of information, as well as safeguarding it against theft, loss, or damage.

ii. All audit team members must have a valid Non-Disclosure Agreement (NDA) in place with their employer organization.

Additionally, depending on the specific project requirements, they may also be required to sign a separate NDA with the auditee organization, with the employer organization being duly informed of such an arrangement.

iii. The resources must understand and ensure there is no conflict of interest.

iv. The resources must have experience and maturity in interacting with senior management and creating trust.

v. The resources must have adequate competency in:
   a. Security Technologies
   b. Security Processes
   c. Security Controls
   d. Security Trends
   e. Fact Collection
   f. Reporting

vi. Auditing Organization must only deploy manpower declared to CERT-In in Snapshot Information Form published on CERT-In's website(https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/Empanel_org.pdf).

vii. The resources should be courteous, cooperative, and professional.

viii. The resources should demonstrate high standards of ethical practices and professional conduct.

ix. The resources should understand the consequences of their actions.

x. A continuous capacity-building program for both technical staff and senior management of the auditing organization should be

developed and maintained, focusing on emerging domains and technologies.

10.3 Handling Audit related data:

i. The auditing organization should treat audit-related data as confidential, handle it with due diligence, and protect it from access by temporary staff or staff in transition/retirement. The auditing organization should immediately implement strict access control for any staff in transition, and the auditee should be apprised of any change in this regard.

ii. Auditee related data should be stored only on systems located in India with adequate safeguards and should keep the auditee informed of the means & location of storage and seek Auditee's consent, where necessary.

iii. During project engagement, Audit related data should be kept in encrypted form in Auditor's laptop.

iv. Auditing organization should also ensure that data is wiped from auditor's laptop after completion of the project. After wiping the data, auditing organization should also make sure that data cannot be retrieved by any known forensic technique. A certificate to this effect should be formally issued to the auditee organization, confirming that all audit-related data has been permanently and irreversibly deleted in accordance with secure data disposal practices.

v. The Auditing organization may retain the audit reports with adequate safeguards to ensure integrity and confidentiality, after completion of audit and it can be shared on 'need to know basis' with the relevant stakeholders after seeking approval from auditee

organization, when required. The data retained should not include any auditee data other than the audit reports.

vi. Auditee related data should only be retained for specific period of time as in Agreement with the auditee or the guidelines by Regulator and disposed-off as per defined & agreed process. The collection, preservation and disposal of data collected by the auditor should be in accordance with the Agreement entered between Auditor & Auditee. In case no specific period is mentioned in Agreement, the data should be retained by auditing organization for 1 year from completion of project.

vii. The Auditing organization to ensure adherence to "Policy Guidelines for Handling Audit related Data" published on CERT-In's website (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/Policy_Guidelines_Handling.pdf).

viii. Audit report should be clear, precise and comprehensive to include all details of audit process, detailed scope, duration of audit, methodologies/standard used, tools, manual process, findings, prioritization, sampling decisions, manpower involved, exemptions, limitations and other constraints

ix. The audit reports shall be signed only by the manpower declared to CERT-In, as listed in the organization's snapshot information available on the CERT-In website. The report must be signed by the Auditors who conducted the audit. It should then be reviewed and signed by a designated Reviewer who is not part of audit team and is from mid-management, to ensure an unbiased and quality review. Finally, the report must be authorized and signed by the Head of the

Auditing Organization (e.g., Director, Partner, or CEO), certifying the completeness, accuracy, and integrity of the audit findings and recommendations.

10.4 Awareness, Training and Outreach

i. Auditing organizations should arrange in-person sessions for their clients or targeted sector on audit awareness, covering the audit fundamentals of cyber security audits such as audit scope, outcomes, limitations of audits, secure development practices and CERT-In initiatives, directions & guidelines on cyber security.

ii. The Auditing organization must maintain a professional relationship with the auditee organization even after the completion of the audit process to keep auditee organization updated for the latest security developments and to help in implementing the secure environment.

10.5 CERT-In Affiliation and Branding Compliance

i. Ensure that CERT-In is not made or projected to be a part of any contract between auditee and auditing organization.

ii. Auditing organization shall not use the CERT-In logo, nor make any reference to the Auditors association with CERT-In on any publicity material, promotional material or product without the prior written permission of CERT-In. Before CERT-In examines requests for permission, the Auditing organization shall submit the wording and presentation of such information.

iii. Auditing organization may use the words "This Organization is empaneled by CERT-In for providing information Security Auditing Service". No other words shall be used to describe the Auditing organization's relationship with CERT-In without the prior written permission of CERT-In.

iv. It is responsibility of empaneled organization to keep CERT-In updated with Snapshot and Point of Contact (PoC) information.

v. Auditing organizations should share the information about their cyber security initiatives with CERT-In for value addition and disseminate it to boarder community.

vi. The Auditing organization shall indemnify, and keep indemnified CERT-In against all claims, demands, actions, costs, expenses, (including without limitation, damages for any loss of business, business interruption, loss of business information or other indirect loss), arising from or incurred by reason of any third party claims against CERT-In relating to or arising from the performance or non-performance by the Auditing organization of any or all of its obligations under this terms and conditions, as well as its Contract with the auditee.

vii. Empaneled organization should not engage in activities like digital break-in, sub-letting or outsourcing of audit assignment, violating terms & conditions of empanelment and unethical business transactions.

10.6 Sharing of Audit report and Audit metadata with CERT-In

It is mandatory for the auditing organization to provide the information pertaining to audits carried by them to CERT-In within 5 days of completion of audit as per format prescribed by CERT-In from time to time to enable CERT-In to act in the matter(s) of capacity building, audit framework, benchmark, quality control and others measures as may be required. The audit data submitted by the entities will be kept confidential.

11. Quality control of auditing organisations involved in Audit

i. CERT-In at any point in time can be a part of the audit team of the auditing organization to assess the quality and maturity of audit and the same should be communicated clearly in writing to the auditee by the auditing organization.

ii. CERT-In reserves the right to seek/audit information from auditing organizations for any project done within the time frame of the empanelment period.

iii. Auditee organization to provide feedback on the audit conducted to CERT-In as well as to auditing organization on completion of the audit. Feedback/complaints to CERT-In would help improve the quality of selecting auditing organizations in future. It is both an auditee organization's right and duty to provide relevant feedbacks. All feedback/complaints are kept confidential and are acted upon promptly with utmost importance. Auditee Feedback form may be requested from empanelment@cert-in.org.in

iv. In case of any adverse feedback from auditee organization/ agencies or any lapses in audit assignments are observed by / reported to CERT-In, actions as per Deter and Punish Framework published by CERT-In (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In >https://www.certin.org.in/PDF/RoD_Interaction_session_website.pdf) may be taken without any reminder or notice.

v. To ensure the quality of audits, auditee organizations are advised to follow practices detailed under Section 12: "Selection of Auditor".

12. Selection of Auditor

12.1 Utilizing Snapshot information for Shortlisting Auditing Organizations

i. The snapshot information of skills and competence of CERT-In empaneled auditing organizations published on CERT-In's website should be utilized by the organizations or sectoral regulators to identify and select the auditing organizations by mapping their requirements with the competence of auditing organizations.

ii. Information about the CERT-In empaneled auditing organizations is available at CERT-In website. The information provided on the CERT-In website can help the auditee organization with respect to the following:

a. Evaluation of manpower and skillset details of an auditing organization.

b. Experience of an auditing organisation relevant to information security audits.
Categories of information security audit conducted by the auditing organization.

c. Information security audits carried out by an organization in last 12 months (sector-wise).

d. Category-wise number of audits conducted by an organization in last 12 months based on data provided by the auditee organization.

e. Technical manpower deployed for audits by an organization with details.

f. Tools used in various audit.

12.2 Selection Process and Evaluation by Auditee

i. The Auditee organizations should interview and select the resources aligned by auditing organizations for competency and experience with respect to the scope of Audit.

ii. Auditee organizations need to verify the technical credentials of the manpower deployed for the audit at their end in line with the qualification requirement mentioned at "Guidelines for applying for Empanelment" published on CERT-In's website (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/InfoSecAuditorsEmpGuidelines.pdf).

iii. Auditee organizations must verify the identity, official identity cards/ government issued documents and designations of the auditing team to ensure that the individuals conducting the audit are legitimate and authorized. Auditing organizations should not field freelancers, interns, freshers, moonlighters, third party consultant or employees who are serving their notice period and the auditee organizations should verify compliance.

iv. While selecting an auditing organization, it is the responsibility of the auditee organization to check the domain of audit conducted, previous audits conducted and other relevant details. Auditee organization should have a clear understanding of the auditing organization's audit methodology, tools used, experience in the relevant domain and all available alternatives like other competent organizations before selecting.

12.3 Resource Vetting and Deployment Standards

i. The resources must have undergone a background check before employment by the auditing organizations. In case of employees moving from one CERT-In empaneled organization to another, a NOC / Relieving Letter shall be required from the previous organization as part of background check and revised snapshot information has to be communicated to CERT-In.

ii. Background verification of individual auditors/employees is the sole responsibility of the auditing organizations. The auditing organization is required to conduct background checks both prior to and, if necessary, following employment.

iii. Auditing Organization must only deploy manpower declared to CERT-In in Snapshot Information Form published on CERT-In's website(https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/Empanel_org.pdf). CERT-In reserves the right to verify/audit such information independently or from the auditing organization or the auditee organization.

12.4 Contractual Guidelines and Contingencies

i. Contracts for the audit of applications especially those are critical or have high user reach, should be awarded by auditee organizations for a period of 2–3 years to enable continuous audits at a defined frequency.

ii. If the credibility of the auditing organization is unclear, auditee organization must make sure that the contractual agreement allows the auditee organization to stop the audit and choose

another auditing organization within a reasonable duration of time in order to avoid financial losses on both ends.

13. Planning the Audit

13.1 Guidelines for Auditee Organizations

13.1.1 Defining and finalizing audit scope

Below mentioned points must be taken into consideration while finalizing the scope of Audit:

a) The auditee organisation should define the complete and comprehensive scope for the audit. The scope of audits should include audit of entire cyber infrastructure including system, applications (both Web/Mobile), software, network infrastructure, Operational Technology (OT) / Industrial Control Systems (ICS) environment, cloud architecture, Application Programming Interfaces (APIs), database and hosting infrastructure, code review, application security, data Security, testing of Incident response capability of the auditee.

b) Scope of audit should be clearly defined by auditee organization in consultation with auditing organization.

c) The scope must be derived from the consolidated and updated asset inventory of the organization. The asset inventory should be reviewed and updated periodically by the IT team.

d) The scope to be submitted to the auditing organisation must be vetted by the internal audit team in consultation with CISO.

e) The auditee organization should provide a comprehensive scope for the audit, ensuring that assets related to the testing / UAT, development, and production environments are included to achieve complete audit coverage.

f) Third-party risk assessment/vendor risk assessment /supply chain risk assessment should be part of scope.

g) The scope of work should clearly specify the requirement to conduct follow-up audits as part of the engagement.

13.1.2 Audit Frequency and Trigger Conditions

i. The cyber security audit should be conducted at least once in a year. The sectoral regulators may decide to increase the audit frequency based on the size of the organization, the criticality of the assets being audited and the complexity of the adoption of digital infrastructure etc.

ii. The above-mentioned frequency may be treated as the minimum frequency and organizations may opt to conduct audits more frequently depending on its risk appetite and criticality of operations and assets.

iii. All changes to the system or application must undergo a formal change management process. Each change should be classified as either a 'Minor Change' or a 'Major Change'. Minor change (low-risk, non-critical) require standard change management processes but do not need a cyber security audit. Major change (high-risk, impactful to security) such as system overhauls, technology migrations, or configuration adjustments that affect sensitive data or critical infrastructure must undergo a cyber security audit to evaluate potential vulnerabilities, ensure compliance, and mitigate security risks before implementation.

iv. Audit should be performed after every major change in infrastructure and application, based on the criticality involved.

v. Audits should be performed even if there is no major change in infrastructure at periodic interval of time to remediate and eliminate the risk from new vulnerabilities. Periodicity of audits should be decided based on the criticality of cyber assets.

13.1.3 Identification and Inclusion of Critical Assets

i. The critical databases/applications need to be identified by the auditee organizations and it must be ensured that the identified critical databases/applications are included in the scope of cyber security audits.

ii. For the identified critical databases, the information security audit should include, but not limited to, database configuration audit.

iii. For the identified critical applications, the information security audit should include, but not limited to, DAST (Dynamic Application Security Testing) and SAST (Static Application Security Testing). Additionally, when procuring the application, the auditee organizations should require that the software developer and/or system integrator supplying the software, perform Static Application Security Testing (SAST). This requirement should be clearly stated in the RFPs and tenders.

13.1.4 Audit Team Planning and Stakeholder Coordination

i. In case any of the activities to be audited in the auditee organization are outsourced, auditee organization must ensure that relevant personnel from outsourced organization are available at the time of audit. The auditing organization's responsibilities need to articulate not just the audit tasks, but also the documentation of their activities, reporting their actions and modus operandi.

ii. A Technical team should be assigned as point of contact by the auditee organization for assisting and monitoring the auditing organization during the audit and the details of the technical team should be shared with the concerned auditors. Auditee organization should assure and schedule regular interaction of technical team with auditors.

13.1.5 Planning for Hosted and Third-Party Infrastructure

i. In cases where a service or website is hosted on a web server owned by another organization, the responsibility for information security auditing of the web server, its operating system, the web hosting application software, and any backend database application software lies with the organization that owns and operates the server, as the website content owner does not have access to or control over these assets. However, since the data and software related to the website are managed by the organization owning the website content, it is their responsibility to ensure that these components are audited by a CERT-In empaneled information security auditing organization.

ii. The organization owning the website content may select any auditing organization from the list of CERT-In empaneled information security auditing organizations, in accordance with its internal rules, procedures, and financial guidelines, to carry out the audit. The audit report provided by the selected auditing organization should explicitly certify that the audited web application including backend databases and scripts, if any, are free from vulnerabilities and malicious code that could be exploited to compromise or gain unauthorized access, including escalated privileges, to the web server hosting the website.

13.1.6 Secure Handling of Reports and Data

A well-defined mechanism must be in place which clearly states the procedure in which the report would be stored and destroyed after the completion of audit by the auditing organization. Thus, the mechanism should be designed in such a way that it confirms the following:

a) Secure handling of report and data at transit.
b) Secure handling of report and data at rest.
c) Disposal time of report and related information by auditing organization.

13.1.7 Audit Contracts, Agreements and Governance

i. The contract should include clear identification of the following:
   a) Audit criteria and standard (Mutually agreed upon by the parties) to discovery all known vulnerabilities based on the comprehensive standards/frameworks like ISO/IEC, Cyber Security Audit Baseline Requirements, CSA Cloud Controls Matrix (CCM) for Cloud Security, Open Source Security Testing Methodology Manual (OSSTMM3), OWASP Web Security Testing Guide for web application security testing, OWASP Application Security Verification Standard (ASVS) for establishing and verifying application security controls, the OWASP Mobile Security Testing Guide (MSTG) for mobile app audits OWASP DevSecOps Maturity Model for assessing CI/CD pipeline security along with applicable regulatory framework and directions & guidelines issued from time to time by agencies such as CERT-In, Government and regulatory bodies.
   b) Audit plan with timelines (Mutually agreed upon by the parties).
   c) Audit tasks.

d) Documentation requirements.

e) Audit Support requirements.

f) Reporting Requirements: Structure, content and secure handling of final deliverable (such as audit reports) should be mutually agreed by auditee and auditing organization.

g) The clause to revalidate the audit observations after the compliance window mentioned in the IS audit policy of the respective auditee organization.

ii. A Non-Disclosure Agreement (NDA) must be signed by the Information Security Auditing Organization prior to the commencement of any audit activities. The auditing organization and its auditors are ethically and contractually obligated to maintain the confidentiality of the auditee's information and security testing results. NDA template is available at CERT-In's website (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-in.org.in/PDF/NON-Disclosure_Agreement.pdf). In addition to the NDA, if the auditee organization wishes to incorporate provisions addressing penal & legal liabilities, such clauses may be included directly in the contract between the auditee and the auditing organization, and may also extend to individual auditors responsible for conducting the audit.

iii. Escalation Matrix should be defined as part of Audit contract in case of repeated vulnerabilities.

13.1.8 Reference Standards and Initial Guidelines

i. 'Cyber Security Audit Baseline Requirements' document published on CERT-In's Website (https://www.cert-in.org.in/->Cyber Security Assurance->Empanelment by CERT-In-> https://www.cert-

in.org.in/PDF/CyberSecurityAuditbaseline.pdf) should be used by auditees and auditing organizations to build their audit program.

ii. Guidelines and directions issued by CERT-In and regulators to be included as part of scope of audit by default.

13.2 Guidelines for Auditing Organizations

13.2.1 Planning Legal and Confidentiality Requirements

i. Ensure a formal Non-Disclosure Agreement is signed with the Auditee and is in place prior to start of work.

ii. Regardless of the existence of a Non-Disclosure Agreement, the security auditing organization is ethically bound to maintain confidentiality and ensure non-disclosure of the auditee's information and security testing results.

iii. Auditing organizations must inform the auditee organisation, prior to the commencement of the audit assignment, about the requirement to share audit metadata and audit reports with CERT-In within five days of audit completion.

13.2.2 Planning the Audit Team and Tool Authorization

i. The information regarding audit team selected for conducting audit should be shared with the auditee and a documented approval regarding the same should be procured before the formal commencement of audit.

ii. The test plan shared by auditing organization must include both calendar time and man-hours.

iii. Ensure that a list of tools planned to be installed is provided to auditee organization along with a written confirmation that the

auditing organization is not violating any IPR or license norms while using and installing the tools.

iv. The auditing organization must have a thorough understanding of the tools they use, including their origin and functionality. These tools should be tested in a controlled test environment prior to deployment on the auditee's systems. The results of such testing must be formally reviewed and approved by an authorized representative of the auditee organization.

v. Appropriate written approvals must be obtained prior to conducting any penetration tests, and the installation of tools should be carried out in the presence of the auditee's system administrator.

13.2.3 Planning Audit Scope and Objectives

i. In order to ensure clarity about the deliverables, below mentioned points must be communicated clearly by the auditing organization to the auditee organization before the commencement of the Audit:

a) Scope of audit shall clearly define the type of audit to be conducted i.e. VAPT (Vulnerability Assessment Penetration Testing), EAPT (External Attack Penetration Testing), DLA (Device Level Audit), Configuration Audit, Process Audit, Mobile Application Security Audit, Web Application Security Audit, API Security Audit, Compliance audit etc.

b) Format of the Reports

c) Standards or Frameworks to be used for conducting audit

d) Assets covered in the scope

e) Handling & retention of auditee data

f) Timeline of the assessment phase

g) Requirement to share audit metadata & reports with CERT-In

ii. Below mentioned points must be taken into consideration while finalizing the scope of Audit:

a) Auditing organization may advise auditee organization to finalize the scope derived from centralized asset inventory to ensure that all the assets are covered in the scope.

b) Auditing organization may advise auditee organization to explicitly mention the date up to which the scope / asset inventory has been updated and this date must be reflected in the audit reports.

c) Version-specific details of web and mobile applications must be explicitly mentioned in the audit scope and report.

iii. Audit should not be performed just for the sake of compliance, but to secure the cyber infrastructure so as to protect the interest & goals of the auditee organization.

13.2.4 Planning Stakeholder Communication and Clarity

i. Ensure that there is no 'expectation gap' in the conduct of the audit. The 'expectation gap' refers to the difference between what the auditee perceives or expects from the audit and what the audit professionals understand the engagement to entail. This gap should be reduced or eliminated by clearly explaining, at the outset, the audit process, required artifacts, and expected deliverables.

ii. The auditing organization should provide clear communication to the auditee organization regarding any exemptions, limitations, and other constraints related to the audit.

13.2.5 Planning Report Handling and Distribution

A report distribution list comprising the official email IDs of designated auditee-side contacts should be obtained prior to report distribution. Additionally, the mobile number of the designated

contact should be collected for securely sharing passwords related to password-protected reports. Both the audit reports and their passwords must be shared exclusively with the authorized contact.

13.2.6 Planning for Risk Escalation and Issue Resolution

There should be a well-defined escalation matrix both for the auditee organization and auditing organization for addressing any problem encountered during the audit process which should be shared with respective authorities.

13.2.7 Planning Remote and High-Risk Test Scenarios

i. In case of remote testing, the identity of the auditor with mobile number and/or IP addresses must be disclosed and formal written permission must be obtained from the auditee organization, clearly outlining the tasks to be performed.

ii. Specific written permissions must be obtained from the auditee organization before conducting tests that involve survivability failures, denial-of-service (DoS), process testing, or social engineering.

iii. The auditing organization must notify the auditee organization in the event of any changes to the audit plan, change in the source test venue, identification of high-risk findings, or prior to conducting new, high-risk, or high-traffic tests. The auditee should also be informed if any testing issues arise. Additionally, the auditing organization should provide progress updates to the auditee at reasonable intervals.

14. Agreeing on the Terms of Engagement and Revisions to the Scope

14.1 Documentation of the Engagement Agreement

i. Before commencing a cyber security audit, it is essential to formally agree upon the terms of engagement between the auditing and auditee organisation. This agreement ensures clarity of purpose, establishes mutual expectations, and defines the responsibilities of all parties involved. A well-documented engagement agreement serves as the foundation for an effective and efficient audit process.

ii. The agreed-upon terms must be formally documented in an audit engagement letter. This document must be reviewed and signed by authorized representatives from both the auditing and the auditee organization. It serves as a binding reference point throughout the engagement.

14.2 Revisions to the Scope

It is recognized that, during the course of the audit, changes in circumstances or new findings may necessitate a revision to the originally agreed scope. In such cases:

a) Revisions must be proposed in writing, with justification for the change. Both parties must evaluate the impact of the revision on audit timelines, resource allocation, and deliverables.

b) Any changes must be approved by authorized representatives and documented as an addendum to the audit engagement letter or through formal amendment procedures.

c) The revised scope must be communicated to all relevant stakeholders to ensure alignment and continued cooperation.

14.3 Criteria for Revisions to the scope

i. Discovery of previously unidentified systems or processes that present significant risk.

ii. Changes in organizational structure, ownership, or regulatory environment.

iii. Security incidents or breaches occurring during the audit period.

15. Performance of the Audit

15.1 Guidelines for Auditee Organizations

15.1.1 Preparing the Audit Environment

i. To prevent a temporary increase in security measures solely for the duration of the audit, the auditee organization should limit notification about the auditing/testing to key personnel only. It is the auditee organization's discretion to identify who these key individuals are; however, they are generally expected to include personnel at the policy-making level, as well as managers responsible for security processes, incident response, and security operations.

ii. The auditee organization should refrain from implementing any unusual or major network changes during the auditing or testing period.

15.1.2 Managing Access and Testing Credentials

If privileged testing is necessary, the auditee organization must provide only temporary access such as login credentials, access tokens, certificates, or secure ID numbers and must ensure that all such privileges are revoked immediately upon completion of the audit.

15.1.3 Monitoring Audit Execution

i. The auditee organization must ensure that the tests agreed upon in the audit contract are being properly executed by the auditing organization, and that the prescribed timelines are adhered to, through the scheduled progress meetings.

ii. The auditee organization should actively track the closure of the assessment phase, re-validation phase, and overall audit completion.

15.1.4 Adhering to Regulatory Guidance

Auditee organization must implement the guidelines and advisories issued by CERT-In and/or Regulator from time to time in their auditing program.

15.2 Guidelines for Auditing Organizations

15.2.1 Pre-Audit Preparation and Compliance

i. A pre-audit discussion on the scope of work must be held between the auditing and auditee organizations to eliminate ambiguities, and ensure alignment with the applicable comprehensive standards and frameworks relevant to the domain and regulatory environment.

ii. The auditing organization must ensure that personnel with appropriate expertise and experience specific to the domain or type of audit are assigned to the engagement.

iii. The auditing organization must revalidate observations from the previous audit cycle, and any unresolved issues should be recorded as repeat observations in the current audit cycle.

iv. Organization must include the verification of compliance to CERT-In direction "Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet"

dated 28 April 2022 in every audit assignment and findings along with relevant evidences should be included in the audit report. Organizations may refer the method of verification document "Method of verifications to compliance with CERT-In Directions issued on 28.04.2022" available on CERT-In website at https://cert-in.org.in/PDF/Methods_of_Verification.pdf.

v. CERT-In updates, advisories and vulnerability notes should be incorporated in the audit practices.

vi. Auditing organizations must comply with all applicable regulations, acts and circulars issued by the government and regulators concerning data security & privacy.

vii. An official exchange of designated Points of Contact (PoCs) should be established between the auditing organization and the auditee organization. This ensures seamless coordination, clarity in communication, and regular interaction before, during, and after the audit process.

15.2.2 Conducting Secure and Ethical Testing

i. When dealing with high-risk vulnerabilities such as discovered breaches, a responsible and ethical approach. These vulnerabilities should be assessed and reported immediately to auditee organisation & CERT-In.

ii. Explicit written permission must be obtained from the auditee organization prior to conducting Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), or flood testing over the Internet to prevent disruption of services.

iii. Social engineering and process testing should be conducted in a controlled and ethical manner. When targeting general staff

(e.g., untrained or non-security personnel), such testing must utilize anonymized or statistical techniques—ensuring no individual is personally identified or penalized. The purpose is to evaluate overall awareness and the effectiveness of security processes, not to single out individuals.

Social engineering and process testing must only target group of employees explicitly included within the agreed audit scope. These tests must not involve external entities such as customers, business partners, vendors, or other third parties, unless specific written consent is obtained from the target organization. This ensures that all testing remains ethical and legally compliant.

iv. In critical environments where availability is a top priority, testing should be conducted in a passive manner to avoid any potential downtime or service disruption.

15.2.3 Managing Testing Environment and Approvals

i. The auditing organization must clearly specify the environment such as Test, Development, UAT, Pre-Production, or Production, in which the application has been tested during application security audit.

ii. The auditing organization is required to audit and test the website on the staging server or testing environment provided by the hosting service provider prior to issuing the Audit Certificate. Application hash values and version numbers must be obtained from the auditee and included in the audit report.

15.2.5 Ensuring Quality, Timelines, and Confidentiality

i. The auditing organization must ensure that all timelines and commitments made to the auditee organization are strictly adhered to.

ii. The security and confidentiality of auditee data must be effectively managed. Well-defined and documented procedures should be established for handling auditee data both during and after the audit.

iii. The auditing organization should implement the maker-checker concept to enhance the quality and effectiveness of security assessments. A separate verification team (checker) should be deployed to review and validate the work performed by the audit team (maker).

15.2.6 Incident Management and Escalation

The auditing organization should have an Incident Management Policy and related processes in place, including a clearly defined escalation matrix and procedures for addressing non-compliance. This incident response process should be shared with the auditee organization.

15.2.7 Review and Coordination

Regular meetings should be conducted between the auditing organization and designated representatives (SPOCs) of the auditee organization to review audit progress, with the objective of assessing and enhancing audit efficiency.

16. Forming an Opinion, Conclusion and Reporting

16.1 Drafting and Structuring the Report

i. Audit report format should be mutually agreed upon (Auditee organization and Auditing organization) and finalized before commencement of the audit.

ii. Audit report should be clear, precise and comprehensive to include all details of audit process, detailed scope, duration of audit, methodologies/standard used, tools, manual process, findings, prioritization, sampling decisions, manpower involved, exemptions, limitations and other constraints.

iii. All the assets provided in the scope by auditee organization must be mentioned in the report.

iv. Report versions – Draft / Final, etc. with date of issuance of each of them to be maintained and captured in the audit report.

v. Audit-related artifacts, such as hash values, versions, and timestamps, be captured by the auditee organization and shared with the auditing organization. These details should be prominently featured in the audit certificate and reports.

vi. The audit reports shall be signed only by the manpower declared to CERT-In, as listed in the organization's snapshot information available on the CERT-In website. The report must be signed by the Auditors who conducted the audit. It should then be reviewed and signed by a designated Reviewer who is not part of audit team and is from mid-management, to ensure an unbiased and quality review. Finally, the report must be authorized and signed by the Head of the Auditing Organization (e.g., Director, Partner, or CEO), certifying the completeness, accuracy, and integrity of the audit findings and

recommendations. The audit certificate must be signed by both the Lead Auditor and the Head of the Auditing Organization.

16.2 Executive Summary and Risk Categorization

i. The audit report should include an executive summary providing a concise overview of the audit findings, including associated risks to the organization and the overall security posture of the audited application or infrastructure. This summary is intended for the board members or top management of the auditee organization. The executive summary should translate the technical findings into relevant business risks and the overall security posture of the audited application or infrastructure.

ii. Auditors are required to implement both CVSS and Exploit Prediction Scoring System (EPSS) frameworks within their audit reports. The observations/vulnerabilities in the report must be categorized based on the Common Vulnerability Scoring System (CVSS) for severity and supplemented with the Exploit Prediction Scoring System (EPSS) to assess the likelihood of real-world exploitation. Every reported observation / vulnerability shall be mapped with Common Weakness Enumeration (CWE) and Common Vulnerabilities and Exposures (CVE) number.

16.3 Practicality of Remediation and Follow-up Actions

i. Ensure that suggested controls and remedies are practical and implementable.

ii. Vulnerabilities classified as 'critical'/'high' in the severity score are required to be notified by the auditor to the auditee organization during the course of audit on as and when found basis. The same is also to be reported in the Final Outcome Report.

iii. Audit report should mention appropriate timelines for closure of vulnerabilities according to severity.

iv. After remediation actions, follow-up audits should be performed by auditing organizations to verify closure of vulnerabilities and non-conformities highlighted in the previous audit.

v. The Final audit report should be issued after the closure of vulnerabilities & completion of follow-up audit of the application hosted on production environment. If the audit scope is limited to the staging platform, the report must explicitly state that the audit was not conducted on production environment.

16.4 Reporting of High Risk Vulnerabilities

High-risk vulnerabilities such as discovered breaches, vulnerabilities with known high exploitation rates, unmonitored, or untraceable access, or those that may pose an immediate risk to life, must be reported to the auditee immediately upon discovery, along with a recommendation for a practical solution.

16.5 Report Delivery and Secure Communication

i. The auditing organization should use only official email IDs for sharing audit reports and related data with the auditee organization.

ii. The audit outcome & related matters should only be communicated to the specified Point of Contact (PoC) of the auditee organization. The audit outcome should only be shared using secure methods such as use of passwords, encryption etc.

iii. All communication channels for delivery of report are end to end confidential.

16.6 Data Handling and Disclosure Guidelines

i. The sharing and disclosure of auditee-related data should be done with the prior consent of the auditee organization. However, disclosures mandated by law or required by designated regulatory bodies or competent authorities in India (such as CERT-In) may be made by the auditing organization without additional consent. The auditee/project-related data shall not be shared with or disclosed to any overseas entity or partner, unless specifically authorized in writing by the auditee organization.

ii. In case of the incidents where client audit related data is leaked to unauthorized entity (intentionally or unintentionally), the auditing organization should inform the auditee about the incident and take all necessary actions to address the incident as may be required.

17. Communication with those Charged with IT Governance

i. The auditing organization will need clear and unambiguous direction from auditee management (written rules of engagement), clearly defined scope for security audit and input on what is required for planning & assessment, requirement analysis, test execution & analysis, results and documentation.

ii. The audit report should be presented to the top management of the auditee organization by the auditing organization.

iii. Entry and Exit conferences should be organized and attended by the senior management of the auditee organization to ensure alignment and commitment throughout the audit process.

The entry conference is crucial for setting clear expectations and ensuring a smooth initiation of the audit. During this meeting, the audit's scope, objectives, timeline, and key responsibilities should be thoroughly discussed and agreed upon, ensuring both parties are aligned on the process. A formal presentation should be delivered to the organization's Board and senior management during onboarding, clearly outlining the auditor's understanding of the scope, the audit methodology to be adopted, key phases of the engagement, and expected timelines. This helps establish transparency, builds confidence, and ensures that the audit begins with mutual understanding and buy-in at the highest levels.

The exit conference serves as a structured forum for the auditing organization to present preliminary findings, highlight key risks, vulnerabilities, and areas of concern identified during the audit. A detailed presentation should be made covering audit observations, the organization's overall security posture, and associated risks, to

enable informed decision-making. Recommendations for remediation should be reviewed, and the auditee's questions or concerns must be addressed to ensure full understanding. The exit conference also provides an opportunity to outline the next steps, including agreed-upon remediation actions and timelines for resolution. This ensures that the audit concludes formally with a clear and actionable roadmap for addressing the identified issues.

iv. The auditing organization should maintain regular contact with the auditee organization even after the audit assignment is completed, as part of a professional relationship. A communication channel should be established to inform or alert the auditee about the latest developments in cyber security that are relevant to their environment.

18. Audit Evidence and Documentation

i. Auditee organizations must seek the working notes upon completion of the audit (provisions for the same should be included in the audit contract) and should ask for audit evidence collected during the assessment be submitted as an appendix along with the final audit report.

ii. In system or compliance audits, artifacts and evidence demonstrating both compliance and non-compliance with controls should be captured and documented by the auditing organization in the audit report.

iii. All the observations made during the audit are well supported with objective evidences and all evidences are compiled carefully and correctly with the report. All the evidence gathered during the process of audit is presented in a manner that the decision makers are able to use them effectively in making credible risk-based decisions.

iv. Audit evidence must be stored securely, with access restricted to authorized personnel only. Proper measures (encryption, access controls, etc.) must be implemented to ensure confidentiality, integrity, and availability of the evidence throughout the audit lifecycle.

v. The auditee organization may request clarifications or justifications for any evidence presented, and the auditing organization must respond within a mutually agreed timeframe.

vi. In case, the scope is related to digital forensic investigation, then, in case such forensic investigation faces constraints due to unavailability/ inadequacy of evidence/ logs then the audit report should explicitly bring out the same and recommend log details to be captured. The report may also encompass a confirmation status to verify the resolution of immediate issues identified in the Root Cause Analysis

(RCA), ensuring that the necessary fixes have been implemented. Additionally, it should detail the completion of cleanup procedures to eliminate any foothold or access points established by threat actors within the infrastructure.

19. Consequences of Non-Compliance to Guidelines and Terms and Conditions of Empanelment

CERT-In has developed and issued a framework to improve quality of audits comprising enabling actions as well as deter & punish mechanism. The framework is available on CERT-In website at https://cert-in.org.in/PDF/RoD_Interaction_session_website.pdf. Following graded actions will be taken by CERT-In and auditee organization in case of adverse reports, violation of these guidelines & terms and conditions of empanelment and poor quality of audits:

a) Move to watch list with warning & written commitment
b) Suspension
c) Debarment as per GFR and De-empanel by CERT-In
d) Penal & Legal Actions

Deter & Punishment matrix –

S.No	Grade: Severity (Moderate to High)	Indicative parameters for Actions	Actions
1.	Move to watch list with warning & written commitment	1. Inadequate closure of Non Compliances (NCs). 2. Lack of relation between Noting & issues raised. 3. Inadequacy of sample details, issues covered, improper conclusions. 4. Violating CERT-In Terms & Conditions (having minor	CERT-In to issue show cause and obtain corrective action report from Auditing Organisations with issue warning along with written commitment.

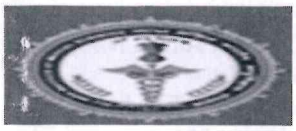
S.No	Grade: Severity (Moderate to High)	Indicative parameters for Actions	Actions
		impact), First adverse report includes missing of maximum 2 vulnerabilities, conflict with auditee, first instance of noncompliance to CERT-In data collection framework, etc	
2.	Suspension	1. Adverse feedback from Auditee regarding technical competency auditor's attributes etc. 2. Repeated failure in respect of audit planning, coverage of audit, Highlighted in CERT-In analysis & observations etc. 3. Issues appearing soon after conduct of audit. 4. Violating CERT-In Terms & Conditions (having major impact), multiple adverse report of missing vulnerabilities, multiple instance of non-compliance to CERT-In data collection framework, etc.	Suspension to be revoked based on satisfactory submission of Corrective Actions and witnessing, if needed

S.No	Grade: Severity (Moderate to High)	Indicative parameters for Actions	Actions
3.	Withdrawal of Empanelment	Auditing malpractices, Substandard services, failure to cover scope of work, etc.	Actions as per GFR and O.M No. F.1/20/2018-PPD dated 2nd November 2021 of Department of Expenditure.
4.	Penal & Legal Actions	Breach of Trust, Digital break-in, Damage & Attempt to damage auditee interests & infrastructure, etc.	As per applicable penal & legal acts / laws

20. Conclusion and Feedback mechanism

i. The objective of these guidelines is to provide a structured, standardized, and practical framework for conducting cyber security audits across organizations. By outlining uniform standards, clearly defining roles and responsibilities, and promoting continual improvement, these guidelines aim to strengthen the overall cyber resilience of the ecosystem. It is expected that these guidelines will serve as a reference for both CERT-In empaneled auditing organizations and auditee entities, ensuring that audits are carried out consistently, effectively, and securely. The document is intended to support the audit process from planning to reporting, ultimately contributing to the broader goal of safeguarding the nation's cyber infrastructure.

ii. CERT-In encourages a collaborative and iterative approach to strengthening the cyber security audit ecosystem. Both auditing organizations and auditee organizations are invited to share their experiences, provide constructive feedback on the audits conducted, highlight any challenges encountered during the audit process, and suggest improvements to these guidelines. Such inputs are vital to ensuring that the audit framework remains practical, relevant, and aligned with evolving technological and threat landscapes. Organizations are requested to submit their feedback or suggestions to empanelment@cert-in.org.in.



Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Appointment of part-time CVO in new AIIMS

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Wed, Dec 17, 2025 at 1:20 PM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **DDA AIIMS PATNA** <dda@aiimspatna.org>
Date: Tue, Sep 23, 2025 at 10:05 AM
Subject: Fwd: Appointment of part-time CVO in new AIIMS
To: Amit Kumar Sinha <amit.sinha@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **Director .** <director@aiimspatna.org>
Date: Mon, 22 Sept 2025, 12:37
Subject: Fwd: Appointment of part-time CVO in new AIIMS
To: DDA AIIMS PATNA <dda@aiimspatna.org>

Sd/-
Prof. (Dr.) Saurabh Varshney
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109

---------- Forwarded message ---------
From: **pmssysection iv** <pmssysectioniv@gmail.com>
Date: Mon, Sep 22, 2025 at 11:59 AM
Subject: Appointment of part-time CVO in new AIIMS
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, <madhabananda@gmail.com>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna

<director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, <drppjoshi@aiimsnagpur.edu.in>, Executive Director Raebareli <edaiimsrbl@gmail.com>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, Sharma, DN <sharmadn@aiims.edu>, Dr.Shakti kumar Gupta <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, <sachimohanty@rediffmail.in>, dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, Dy Director Administration AIIMS, Raebareli <ddaaiimsrbl@gmail.com>, Dr. Pradip Kumar <kpradip10@gmail.com>, <dda@aiimskalyani.edu.in>, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, <dda@aiimsrbl.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, <dda@aiimsbilaspur.edu.in>, Mukesh Kumar <mac.prasad@gmail.com>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, <aps101982@rediffmail.com>, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, Administrative Officer <ao.aiimsmadurai@gmail.com>, <dda@aiimsguwahati.ac.in>, <ddaaiimsawantipora1@gmail.com>
Cc: : <Ak.biswas57@nic.in>, <premprakash.bth@gov.in>, <manoj@ndma.gov.in>, Suprava Poddar <sup15.81997@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officers of PMSSY-IV Section at - ak.biswas57@nic.in; premprakas h.bth@gov.in; manoj@ndma.gov.in; sup15.81997@gov.in;
Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

Letter (171).pdf
88K

No.: Z-28015/51/2024-PMSSY-IV (8287964)
Government of India
Ministry of Health and Family Welfare
(PMSSY - IV Section)
***

Room No:745A, Nirman Bhawan,
New Delhi Dated 22-09-2025

To,

1. Executive Directors of new AIIMS
2. Deputy Directors (Administration) of new AIIMS

Subject: Appointment of part-time CVO in new AIIMS.

Sir/Madam,

It may be noted that part-time Chief Vigilance Officers (CVOs) are being appointed in new AIIMS with the approval of Central Vigilance Commission (CVC). As advised by the CVC, the part-time CVOs appointed at the Institute shall not be associated with procurement, recruitment, tendering and/or security or any such decision-making activity, which has potential conflict of interest.

2. Executive Directors of all new AIIMS are advised to ensure compliance of the above both in letter and spirit.

Yours faithfully,

Digitally signed by
ARUN KUMAR BISWAS
Date: 22-09-2025
11:23:20

(Arun Kumar Biswas)
Under Secretary to the Government of India
Tel: 011-23063848

DDA AIIMS PATNA <dda@aiimspatna.org>

Extension in the period of deputation tenure beyond the initial period of 3 years – reg.

pmssysection iv <pmssysectioniv@gmail.com> Tue, Oct 28, 2025 at 4:26 PM
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, madhabananda@gmail.com, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, drppjoshi@aiimsnagpur.edu.in, Executive Director Raebareli <edaiimsrbl@gmail.com>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, "Prof. Dr. D.K. Singh, Director" <director@aiimsbathinda.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, "Dr.Shakti kumar Gupta" <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, ed@aiimsrajkot.edu.in, edaiimsrajkot2020@gmail.com, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, sachimohanty@rediffmail.in, "Sharma, DN" <sharmadn@aiims.edu>
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, "Dy Director Administration AIIMS, Raebareli" <ddaaiimsrbl@gmail.com>, "Dr. Pradip Kumar" <kpradip10@gmail.com>, dda@aiimskalyani.edu.in, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, dda@aiimsbilaspur.edu.in, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, aps101982@rediffmail.com, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, dda@aiimsguwahati.ac.in, raj08642@gmail.com, Mukesh Kumar <mac.prasad@gmail.com>, ddaaiimsawantipora1@gmail.com, ":" <Ak.biswas57@nic.in>, Vaishali Vinayak <vaishali.vinayak@gov.in>, Amit Batra <amit.batra@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officers of PMSSY-IV Section at - ak.biswas57@nic.in; vaishali.vinayak@gov.in; amit.batra@gov.in;

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

2 attachments

Letter (225).pdf
93K

extension guidelines.pdf
3692K

Z-28015/99/2025-PMSSY-IV
Government of India
Ministry of Health and Family Welfare
PMSSY – IV Section
****

Room No. 745-A, Nirman Bhawan, New Delhi
Dated the 28-10-2025

To

Executive Director, all new AIIMS

Subject: Extension in the period of deputation tenure beyond the initial period of 3 years – reg.

Sir,

The undersigned is directed to refer to this Ministry's letter No. Z-28016/88/2025-PMSSY-IV(8335252) dated 15.05.2025 & 21.05.2025 (copies enclosed) and to convey that all new AIIMS may immediately relieve the concerned officer from the deputation post in case NOC from his/her parent organization for extending the deputation tenure is not received before the date of completion of deputation tenure.

2. This issues with the approval of Secretary (HFW).

Yours faithfully,

Digitally signed by
ARUN KUMAR BISWAS
Date: 28-10-2025
16:06:31

(Arun Kumar Biswas)
Under Secretary to the Government of India
Tel:011-23063848
ak.biswas57@nic.in

Copy to : Deputy Director (Administration), all new AIIMS

No. Z-28016/88/2025-PMSSY-IV(8335252)
Government of India
Ministry of Health and Family Welfare
(PMSSY - IV Section)
***

Room No: 745A, Nirman Bhawan, New Delhi

Dated 21-05-2025

To

Executive Director(ED), of all new AIIMS

Subject: Extension in the period of deputation tenure beyond the initial period of 3 years in new AIIMS - reg.

Sir/ Madam,

Reference is invited to this Ministry's letter of even no. dated 15.05.2025 (copy enclosed) on the subject mentioned above.

2. All new AIIMS are requested to submit the details of cases of overstayal, where the officer is continuing on deputation beyond the initial tenure of 3 years without approval of the competent authority. i.e. Secretary(HFW), for consideration by the Ministry, by 31.05.2025 positively.

3. The details to be provided by the institute shall include the following:

i. Copy of the willingness indicated by the officer for extension of deputation tenure.

ii. Copy of NOC provided by Cadre Controlling Authority.

iii. Vigilance status, including details of complaints, if any received against the officer.

iv. Copy of notings of the Institute processed for unilaterally extending the deputation tenure.

v. Copy of the order issued by the Institute for extension of the deputation tenure.

4. This issues with the approval of the Competent Authority.

Encl: As above

Yours faithfully,
Digitally signed by
ARUN KUMAR BISWAS
Date: 21-05-2025
14:54:52
(Arun Kumar Biswas)
Under Secretary to the Government of India
Email: ak.biswas57@nic.in

Copy to: Dy. Director (Admin), all new AIIMS

679

Z-28015/88/2025-PMSSY-IV(8335252)
Government of India
Ministry of Health & Family Welfare
(PMSSY-IV Section)

Room No. 745-A, Nirman Bhawan, New Delhi
Dated the 15-05-2025

To,

Executive Director (ED), of all new AIIMS

Subject: Extension in the period of deputation tenure beyond the initial period of 03 years in new AIIMS.

Sir/ Madam,

Reference is invited to the 'Consolidated guidelines on deputation/foreign service for Central Government employees' issued by the Department of Personnel and Training vide OM No. DOPT- 1726140763694 dated 28.03.2024. The guidelines provide *inter alia* the following:

> *"8.2 In case where the period of deputation/foreign service prescribed in the RRs of the ex-cadre post is 5 years or less than 5 years, the borrowing Ministry/Department/Organization may grant extension upto the 6th year after obtaining orders of their Secretary (in the Central Government)/ Chief Secretary (in the State Government)/ equivalent officer (in respect of other cases) and for the 7th year with the approval of the Minister of the borrowing Ministry/Department and in respect of other organizations with the approval of the Minister of the borrowing Ministry/Department with which they are administratively concerned.*
>
> ...
>
> ...
>
> *12. The deputationist officer is deemed to have been relieved on the date of expiry of the deputation period unless the competent authority has with requisite approvals, extended the period of deputation, in writing, prior to the date of its expiry. It will be the responsibility of the immediate superior officer to ensure that the deputationist does not overstay. In the event of the officer overstaying for any reason whatsoever, he/she is liable to disciplinary action and other adverse Civil/Service consequences which would include the period of unauthorized overstay not being counted for service for the purpose of pension and that any increment due during the period of unauthorized overstay being deferred with cumulative effect, till the date on which the officer rejoins his parent cadre."*

2. In terms of the extant instructions, the appointments to non-faculty posts in new AIIMS on deputation basis are being made for a period of 03 years. In terms of DoPT's aforesaid OM dated 28.03.2024, extension of deputation tenure upto 6th year requires approval of Secretary (in the Central Government)/Chief Secretary (in the Central Government)/equivalent officer (in respect of other cases). It has been

680

observed that some new AIIMS have been extending the deputation tenure of various posts beyond the initial approved tenure without obtaining the prior approval of Secretary (HFW). The posts of Chief Executive officer in new AIIMS is being operated at Level 15 of the pay matrix as Executive Director, and thus cannot be equated with the post of Secretary to the Government of India, the level at which the cases for extension in deputation tenure are to be decided in terms of DoPT's aforesaid OM dated 28.03.2024.

3. It is, accordingly, clarified that in compliance with DoPT's aforesaid OM dated 28.03.2024, all cases for extension in deputation tenure in new AIIMS, beyond the initial period 03 years upto 06th year, require prior approval of Secretary (HFW).

4. The instructions contained in para 12 of DoPT's OM dated 28.03.2024 shall apply to unauthorized overstay where the officers are continuing on deputation posts beyond the initial period of 03 years without prior approval of the competent authority.

5. All Executive Directors of AIIMS are advised to comply with the above OM of DoPT in letter and spirit and forward all cases of extension on deputation of officials in AIIMS beyond 3 years for consideration and approval of Secretary HFW.

6. Overstayal of officers in the Institutes beyond the period of deputation without approval of the Competent Authority will be viewed seriously. Any approval for extension of deputation beyond 3 years granted at the level of the Institute is to be treated as null and void.

7. This issues with the approval of the Competent Authority.

Encl(1): OM No. DOPT- 1726140763694 dated 28.03.2024

Yours faithfully

Digitally signed by
ARUN KUMAR BISWAS
Date: 15-05-2025
11:32:50

(Arun Kumar Biswas)
Under Secretary to the Government of India
Tel:011-23061343
ak.biswas57@nic.in

Copy to:

i. Deputy Director(Admin) of all new AIIMS

Copy for information to:

i. PSO to Secretary(HFW)

ii. PPS to JS(PMSSY)

Z-28015/88/2025-PMSSY-IV(8335252)
Government of India
Ministry of Health & Family Welfare
(PMSSY-IV Section)

Room No. 745-A, Nirman Bhawan, New Delhi
Dated the 15-05-2025

To,

Executive Director (ED), of all new AIIMS

Subject: Extension in the period of deputation tenure beyond the initial period of 03 years in new AIIMS.

Sir/ Madam,

Reference is invited to the 'Consolidated guidelines on deputation/foreign service for Central Government employees' issued by the Department of Personnel and Training vide OM No. DOPT- 1726140763694 dated 28.03.2024. The guidelines provide *inter alia* the following:

> *"8.2 In case where the period of deputation/foreign service prescribed in the RRs of the ex-cadre post is 5 years or less than 5 years, the borrowing Ministry/Department/Organization may grant extension upto the 6th year after obtaining orders of their Secretary (in the Central Government)/ Chief Secretary (in the State Government)/ equivalent officer (in respect of other cases) and for the 7th year with the approval of the Minister of the borrowing Ministry/Department and in respect of other organizations with the approval of the Minister of the borrowing Ministry/Department with which they are administratively concerned.*
>
> ...
>
> ...
>
> *12. The deputationist officer is deemed to have been relieved on the date of expiry of the deputation period unless the competent authority has with requisite approvals, extended the period of deputation, in writing, prior to the date of its expiry. It will be the responsibility of the immediate superior officer to ensure that the deputationist does not overstay. In the event of the officer overstaying for any reason whatsoever, he/she is liable to disciplinary action and other adverse Civil/Service consequences which would include the period of unauthorized overstay not being counted for service for the purpose of pension and that any increment due during the period of unauthorized overstay being deferred with cumulative effect, till the date on which the officer rejoins his parent cadre."*

2. In terms of the extant instructions, the appointments to non-faculty posts in new AIIMS on deputation basis are being made for a period of 03 years. In terms of DoPT's aforesaid OM dated 28.03.2024, extension of deputation tenure upto 6th year requires approval of Secretary (in the Central Government)/Chief Secretary (in the Central Government)/equivalent officer (in respect of other cases). It has been

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

observed that some new AIIMS have been extending the deputation tenure of various posts beyond the initial approved tenure without obtaining the prior approval of Secretary (HFW). The posts of Chief Executive officer in new AIIMS is being operated at Level 15 of the pay matrix as Executive Director, and thus cannot be equated with the post of Secretary to the Government of India, the level at which the cases for extension in deputation tenure are to be decided in terms of DoPT's aforesaid OM dated 28.03.2024.

3. It is, accordingly, clarified that in compliance with DoPT's aforesaid OM dated 28.03.2024, all cases for extension in deputation tenure in new AIIMS, beyond the initial period 03 years upto 06th year, require prior approval of Secretary (HFW).

4. The instructions contained in para 12 of DoPT's OM dated 28.03.2024 shall apply to unauthorized overstay where the officers are continuing on deputation posts beyond the initial period of 03 years without prior approval of the competent authority.

5. All Executive Directors of AIIMS are advised to comply with the above OM of DoPT in letter and spirit and forward all cases of extension on deputation of officials in AIIMS beyond 3 years for consideration and approval of Secretary HFW.

6. Overstayal of officers in the Institutes beyond the period of deputation without approval of the Competent Authority will be viewed seriously. Any approval for extension of deputation beyond 3 years granted at the level of the Institute is to be treated as null and void.

7. This issues with the approval of the Competent Authority.

Encl(1): OM No. DOPT- 1726140763694 dated 28.03.2024

Yours faithfully

Digitally signed by
ARUN KUMAR BISWAS
Date: 15-05-2025
11:32:50

(Arun Kumar Biswas)
Under Secretary to the Government of India
Tel:011-23061343
ak.biswas57@nic.in

Copy to:

i. Deputy Director(Admin) of all new AIIMS

Copy for information to:

i. PSO to Secretary(HFW)

ii. PPS to JS(PMSSY)

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

Gmail pmssysection iv <pmssysectioniv@gmail.com>

Extension in the period of deputation tenure beyond the initial period of 03 years in new AIIMS.

1 message

pmssysection iv <pmssysectioniv@gmail.com> Thu, May 15, 2025 at 11:46 AM
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, drppjoshi@aiimsnagpur.edu.in, Executive Director Raebareli <edaiimsrbl@gmail.com>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, "Sharma, DN" <sharmadn@aiims.edu>, "Dr.Shakti kumar Gupta" <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, madhabananda@gmail.com, sachimohanty@rediffmail.in
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, Rajeev Sen Roy <rajeevsenroy30@gmail.com>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, dda@aiimsrbl.edu.in, "Dy Director Administration AIIMS, Raebareli" <ddaaiimsrbl@gmail.com>, "Dr. Pradip Kumar" <kpradip10@gmail.com>, dda@aiimskalyani.edu.in, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, dda@aiimsbilaspur.edu.in, Mukesh Kumar <mac.prasad@gmail.com>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, aps101982@rediffmail.com, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, Administrative Officer <ao.aiimsmadurai@gmail.com>, T Ngamlien <t.ngamlien@icg.gov.in>, ddaaiimsawantipora1@gmail.com, Apurva Chandra <secyhfw@nic.in>, Praveen Batra <Praveen.batra@gov.in>, ":" <Ak.biswas57@nic.in>, Vaishali Vinayak <vaishali.vinayak@gov.in>, Amit Batra <amit.batra@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officers of PMSSY-IV Section at - arvind.thakur@nic.in; ak.biswas57@nic.in;, vaishali.vinayak@gov.in; amit.batra@gov.in

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

2 attachments

Letter (284).pdf
103K

Subject_- Consolidated guidelines on deputation_foreign service for central government employees.pdf
804K

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

Government of India
Ministry of Personnel, Public Grievances & Pensions
Department of Personnel and Training
ESTT.(Pay-II)
******

Dated 28 March, 2024

OFFICE MEMORANDUM

Subject:- Consolidated guidelines on deputation/foreign service for central government employees

D/o Personnel & Training (DoPT) had vide OM No. AB-14017/2/07-Estt(RR) dated 29.02.2008 issued consolidated guidelines governing appointments of the Central Government employees to the posts filled on deputation / foreign service.

2. In so far as Central Government employees are concerned, foreign service has been defined as service in which a Government servant received his pay with the sanction of Government from any source other than the Consolidated Fund of India **{ FR 9(7)}**.

3. Instructions contained in the OM referred above cover cases involving appointments under following categories:

[DOPT OM No. AB-14017/2/07-Estt(RR) dated 29.02.2008]

(a) Central Staffing Scheme (CSS)

Central Staffing Scheme (CSS) provides a systematic arrangement for selection and appointment of officers to senior administrative posts at Centre, excluding posts which are specifically encadred within the Organised Group 'A' Services or filled by recruitment through the Union Public Service Commission. Instructions governing various aspects of the Central Staffing Scheme issued from time to time have been consolidated and placed on the official website of DoPT. Matters relating to appointment under Central Staffing Scheme and other related issues are handled in the Office of the Establishment Officer (O/o the EO), DoPT.

[DoPT OM No.DOPT-1705650752584 dated 19.01.2024]

(b) Non-Central Staffing Scheme (Non-CSS)

Appointments to following categories of posts are covered under Non-Central Staffing Scheme:

i. Posts of **Chief Vigilance Officer (CVOs)**. Guidelines/procedure for appointment of CVOs in CPSEs and other organizations under Central Government and their service conditions have been consolidated and placed on DoPT's official website. Matters relating to appointment of CVOs and other related issues are handled in O/o the EO, DoPT.**[DoPT OM No.40/1/2022-EO(CVO) dated 18.11.2022]**

ii. Posts in **Statutory Bodies and Autonomous Institutions wholly or substantially funded or controlled by the Central Government**. Selection to fill these posts is made through Search-cum-Selection Committee process as laid down in DoPT's OM No. AB-14017/11/2004-Estt(RR) dated 30.07.2007 OR as per the approved Recruitment Rules OR as per the statutory provisions for institutions covered by specific statutes (with the approval of ACC for Chief Executives of Joint Secretary or above level). Tenure of these appointments shall be as prescribed under Central Staffing Scheme. Instructions on setting up Search Committees /Search-cum-Selection Committees and related topics have been placed on DoPT's official website.**[AB.14017/24/2022-Estt.(RR) dated 31.08.2022]**

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
about:blank
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

Absorption Rule, appointment to the posts under this category is made through Public Enterprises Selection Board (PESB)/ Search Committee (with the approval of ACC for Joint Secretary and above level posts). Tenure of these appointments shall be as prescribed under Central Staffing Scheme.

iv. Further, in partial modification of the existing instructions governing deputation/foreign service as also para 1.3 of this Department's OM No.AB-14017/2/2007-Estt (RR) dated 29.02.2008, instructions have been issued vide DoPT's OM No.*6/8/2023-Pers.Policy (Deputation/Re-employment) Pt.XV* 15.03.2024 regulating the appointment and other terms and conditions of deputation of Group 'A' officers of the Central Government **to ex-cadre posts under a State Government/UT Administration including PSUs/ Autonomous bodies/Statutory Bodies/ Universities/Local Bodies under the States/UT Administration**.

[DoPT's OM No.6/8/2023-Pers.Policy (Deputation/Re-employment) Pt.XV dated 15.03.2024]

v. Posts in **Constitutional Bodies or Staff Officers of Heads of Constitutional Bodies**. Selection and appointments to the posts under this category is made through Civil Services Board OR on request by name, subject to vigilance clearance and suitability (with the approval of ACC for Joint Secretary and above level posts). Tenure of these appointments shall be as prescribed under Central Staffing Scheme.

vi. Posts in **Statutory Bodies set up by an Act of Parliament or Staff Officers of Heads of such Statutory Bodies**. Selection to the posts below Joint Secretary level shall be made by a Committee under the Chairmanship of Secretary(Personnel) with the approval of MoS(PP). Appointment to Joint Secretary and above level posts shall be made through Civil Services Board and with the approval of ACC. Tenure of these appointments shall be as prescribed under Central Staffing Scheme.

vii. Posts in **Non-permanent, Non-Statutory Bodies with a specific term set up through executive orders/notification by the Central Government** – like Administrative Reforms Commissions, Pay Commission, National Manufacturing Competitiveness Commission, Sachar Committee, Inquiry Commissions etc. Appointment to the posts under this category is made through Civil Services Board (with the approval of Appointments Committee of the Cabinet for Joint Secretary and above level posts). Tenure of these appointments shall be as prescribed under Central Staffing Scheme. If an officer moves from a Central Staffing Scheme post to Non-Central Staffing Scheme post, or vice versa, he/she shall be eligible for an additional tenure of two years, subject to at least two years on either post.

(c) <u>Deputation to International Organisations</u>

Appointments to posts in the following organisations are covered under this category:

(i) UN Organisations

(ii) International Financial Institutions like World Bank, IMF, ADB etc.

(iii) Multilateral organisations of which India is a member, like IAEA, WTO, Commonwealth Organisation, International Court of Justice, SAARC etc.

(iv) Bilateral Bodies set up under the Vienna Convention i.e. Embassies and Bodies set up under them, like USAID, DFID, NORAD etc.

(v) International NGOs or Funding Organisations from which India receives technical / financial assistance like international Red Cross Society, Action Aid, Aga Khan Foundation, Ford Foundation etc.

A Committee under the Chairmanship of Cabinet Secretary with Secretary(Personnel), Finance Secretary will screen all proposals for deputation on foreign service terms of officers of the level of Joint Secretary and above, on a case to case basis, after the proposals have been approved by the Cadre Controlling Authority. Such screening in the case of officers below the level of Joint Secretary will be done by a Committee chaired by the Secretary of the Cadre Controlling Ministry/Department with a member each, not below the level of Joint Secretary from the Department of Personnel & Training and Department of Expenditure. A final decision on the recommendation of the Screening Committee may be taken at the level

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
Generated from eOffice by VAISHALI VINAYAK. SO(VV)-PMSSY-IV. SECTION OFFICER. DOHFW DEPARTMENT on 15/05/2025 11:53 am

of the Prime Minister in the case of officers holding Joint Secretary level posts or above.

For appointments to the posts listed at (iv) above, the Foreign Secretary or the MEA Secretary concerned shall also be a member of the Committee under the chairmanship of Cabinet Secretary for officers of Joint Secretary and above level. For officers below Joint Secretary level, a nominee of Foreign Secretary not below the level of Joint Secretary would be included in the Screening Committee. Further, for appointments to the posts listed at (v) above, concurrence of Ministry of Home Affairs shall be taken. Maximum tenure of appointments under this category shall be 5 years at a stretch.

(d) <u>Autonomous body, trust, society etc. not controlled by the Government or a private body</u>

Appointments in the following bodies are covered under this category:

(i) Registered Societies or Trusts or Foundations or non-profit organisations or NGOs or cooperatives;

(ii) Apex bodies of Industries and Commerce.

For appointments to the posts in such autonomous or private bodies, all the conditions of the following criteria need to be fulfilled:

a. They are functionally autonomous of the Central and State Governments;

b. They are not substantially funded by the Central and State Governments;

c. Central or State Governments do not have powers to give them directions; and

d. They are not companies registered under the Registration of Companies Act.

Procedure for appointment to the posts in these bodies shall be as detailed in para 3(c) above. Maximum tenure of appointments under this category shall be 5 years at a stretch.

(e) <u>Ex-Cadre deputation</u>

D/o Personnel & Training has from time to time issued instructions / guidelines regulating appointment, pay, Deputation (Duty) Allowance, tenure of deputation/ foreign service and other terms and conditions of deputation/foreign service of the Central Government employees to ex-cadre posts under the Central/State Governments/ Union Territories (UTs) Administration/ Public Sector Undertakings (PSUs)/ Autonomous Bodies/ Statutory Bodies/ Universities/ Local Bodies etc. and *vice-versa*.

APPLICATION

2.. These provisions apply to all Central Government employees, who are regularly appointed on deputation/foreign service in accordance with the provisions of the Recruitment Rules (RRs) of the ex-cadre posts, under the same or some other Departments of Central Government or under the State Governments/ UTs Administration/Local Bodies or under Central or State PSUs/Autonomous Bodies/Statutory Bodies etc. set up or controlled by Central/State Governments provided the foreign service under such PSUs/Autonomous Bodies/Statutory Bodies has been permitted in relaxation of appointment on immediate absorption basis. They also cover the cases of regular appointment on deputation/foreign service of employees of State Government/Local Bodies etc. as well as PSUs/Autonomous Bodies/Statutory Bodies of Central/State Governments as per RRs in the Central Government. In short, these instructions cover cases of deputation/foreign service where Central Government is either lending authority or borrowing authority or both.

2.1 However, in partial modification of the existing instructions governing deputation/foreign service as also para 1.3 of this Department's OM No.AB-14017/2/2007-Estt (RR) dated 29.02.2008, **appointment and terms and conditions of deputation of Group 'A' officers of the Central Government to ex-cadre posts under a State Government/UT Administration including PSUs/ Autonomous bodies/Statutory Bodies/ Universities/Local Bodies under the States/UT Administration**, would be regulated as per the revised instructions issued in this regard vide **DoPT's OM No. *6/8/2023-Pers.Policy (Deputation/Re-employment)***

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 01:07 pm
File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
about:blank
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

out in the said OM shall be regulated by the instructions indicated herein.

[DoPT's OM No. AB-14017/2/07-Estt.(RR) dated 29.02.2008; ***DoPT's OM No. 6/8/2009-Estt.(Pay-II) dated 17.06.2010; DoPT's OM No. 2/9/2018-Estt.(Pay-II) dated 12.4.2021*** and ***DoPT's OM No. OM No.6/8/2023-Pers.Policy (Deputation/Re-employment) Pt.XV dated 15.03.2024]***

2.2. However, the following cases are governed by separate set of instructions / guidelines, and they are not covered by these provisions: -

(a) Members of the All India Services and those deputed to posts, whose terms are regulated under specific statutory rules or orders;

(b) Officers appointed on deputation to posts under the Central Staffing Scheme (CSS) for whom separate orders issued from time to time continue to apply;

(c) Deputation to posts operated outside India;

(d) Appointments of a specific category of employees to a specified class of posts, such as appointments made in the Personal Staff of Ministers etc., in respect of which special orders are already in existence. However, the terms and conditions contained herein will apply to those cases to the extent they are not specifically covered under such special orders.

(e) Appointments of the nature of deemed deputation or transfers to ex-cadre posts made in exigencies of service with the specific condition that no Deputation (Duty) Allowance will be admissible - e.g. (i) interim arrangements in the event of conversion of a Government office/organization or a portion thereof into a PSU/ Autonomous Body or *vice-versa*; and (ii) appointments to the same post in another cadre.

[Para 2.1 and 2.2 of DoPT's OM No. 6/8/2009-Estt.(Pay-II) dated 17.06.2010]

SCOPE OF THE TERM 'DEPUTATION/FOREIGN SERVICE' RESTRICTIONS ON TREATING AN APPOINTMENT AS ON DEPUTATION/ FOREIGN SERVICE.

3.1 The terms 'Deputation'/ 'Foreign Service' will cover only those appointments that are made by transfer on a temporary basis provided the transfer is outside the normal field of deployment and is in public interest. The question whether the transfer is outside the normal field of deployment or not will be decided by the authority which controls the service or post from which the employee is transferred.

3.2 The following types of appointments will not be treated as deputation/foreign service for the purposes of these orders:

(a) Appointment of serving employees made either by promotion or by direct recruitment from amongst open market candidates whether on permanent or temporary basis;

(b) Permanent appointment made by transfer/absorption;

(c) Temporary appointment made based on personal requests of employees;

(d) Arrangements necessitated by staff imbalances arising on reorganization of offices on the same or different stations, subject to the specific condition that no Deputation (Duty) Allowance will be admissible in

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8335252)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 am

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
about:blank
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

3.3 A person in a higher Level (in Pay Matrix) shall not be appointed on deputation to a post in lower Level (in Pay Matrix) if the deputation is from Central Government to Central Government and also in cases where the scale of pay and Dearness Allowance (DA) in the parent cadre post and ex-cadre post are similar.

[Para 3.1-3.3 of DoPT's OM No. 6/8/2009-Estt.(Pay-II) dated 17.06.2010]

3.4 However, no appointment on deputation/foreign service shall be made from/to Central Government/an organization where the scale of pay and DA pattern in the parent cadre post and ex-cadre post are dissimilar, if the basic pay in the parent cadre increased by one increment plus Dearness Allowance (s) including interim relief if any, admissible to a person in the parent cadre post exceeds the basic pay plus Dearness Allowance(s) including interim relief, if any, at the maximum of the pay Level in the Pay Matrix/pay scale of the ex-cadre post.

Note: In the revised pay structure under 7th CPC, the maximum of the scale would mean the last cell of any Level in the Pay Matrix.

Illustration:

In case of an appointment on deputation basis, from an organization to an ex-cadre post in the Central Government in Level 7 in the Pay Matrix, where the pay scale and DA pattern of the parent cadre post and ex-cadre post in Central Government are dissimilar, no appointment can be made to such post, if the basic pay in the parent cadre increased by one increment plus Dearness Allowance (s) including Interim Relief, if any, admissible in the parent cadre post exceeds the basic pay at the maximum of the Level 7 of the Pay Matrix i.e. Rs. 1,42,400/- plus Dearness Allowance (s), including Interim Relief, if any.

[DoPT's OM No. 2/9/2018-Estt.(Pay-II) dated 12.04.2021]

EXERCISE OF OPTION.

4.1 An employee appointed on deputation/foreign service, may elect to draw either the pay in the Level (in the Pay Matrix)/Scale of pay of deputation/foreign service post or his/her basic pay in the parent cadre plus Deputation (Duty) Allowance thereon plus Personal Pay, if any. However, in case of appointment of Government employees on deputation/ foreign service to CPSEs, this option will not be allowed, and in such cases their pay will be governed in terms of the orders issued by Department of Public Enterprises vide OM dated 26.11.2008 and clarifications issued thereafter.

4.2 The borrowing authority shall obtain the option of the employee within one month from the date of joining the ex-cadre post unless the employee has himself furnished the option.

4.3 The option once exercised shall be final.

4.4 However, the employee may revise the option under the following circumstances which will be effective from the date of occurrence of the same:

a. When he/she receives proforma promotion or is appointed to non-functional selection grade or up-gradation of scale in the parent cadre;

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm
File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
about:blank
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

c. When the scale of pay/level (in the Pay Matrix) of the parent cadre post based on which his emoluments are regulated during deputation/foreign service or of the ex-cadre post held by the employee on deputation/foreign service is revised either prospectively or from a retrospective date;

d. Based on the revised/same option of the employee, in the event of proforma promotion/appointment to non-functional selection grade/revision/upgradation of scales of pay/level (in the Pay Matrix) in the parent cadre, his/her pay will be re-fixed with reference to the revised entitlement of pay in the parent cadre. However, if the initial option was for the pay scale of the deputation post and no change in option already exercised is envisaged, the pay already drawn in deputation post will be protected if the pay re-fixed is less.

Note: Revision in the rates of DA, HRA or any other allowance either in the parent or borrowing organization shall not be an occasion for revision of the earlier option.

4.5. If the pay of an employee in his cadre post undergoes downward revision, the pay in the ex-cadre post is also liable to be re-fixed based on revised pay and in accordance with the revised option or existing option if the employee does not revise his option.

[Para 4 of DoPT's OM No. 6/8/2009-Estt.(Pay-II) dated 17.06.2010]

PAY FIXATION.

5.1 When an employee on deputation/foreign service elects to draw pay in the Level (in Pay Matrix) attached to the ex-cadre post, his/her pay may be fixed as under:

(i) **Deputation from Central Government to Central Government**:

If the Level (in Pay Matrix) of the ex-cadre post is higher than that of the parent cadre post, an increment shall be given in the Level (in Pay Matrix) of parent cadre post and he/she shall be placed at a Cell equal to the figure so arrived at in the Level (in Pay Matrix) of the excadre post; and if no such Cell is available in the Level (in Pay Matrix) of the ex-cadre post, he/she shall be placed at the next higher cell in that Level. However, if the cell so arrived at after adding an increment is less than the minimum of the cell in the Level (in Pay Matrix), the pay will be fixed at the minimum of the cell in the Level (in Pay Matrix).

In case Levels (in Pay matrix) of the ex-cadre post and the parent cadre post of the employee are identical, the employee would continue to draw his/her basic pay.

(ii) **In case of Foreign Service/Reverse Foreign Service**:

(a) When the Level (in Pay Matrix)/Pay Scale of the post in the parent cadre and that attached to ex-cadre post are based on the same index level and the DA pattern is also same, the pay may be fixed as under (i) above.

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
about:blank
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

is dissimilar to that in the parent organization, pay may be fixed by adding one increment to the basic pay of the substantive post in the parent cadre, (and if he/she was drawing pay at the maximum of the scale, by the increment last drawn) and equating the pay so raised plus dearness allowance (and additional or ad-hoc dearness allowance, interim relief etc., if any) with emoluments comprising of basic pay plus DA, ADA, Interim Relief etc., if any, admissible, in the borrowing organization and the pay may be fixed at the stage in the Pay Scale/ Level (in Pay Matrix) of the ex-cadre post at which total emoluments admissible in the ex-cadre post as above equal the emoluments drawn in the parent cadre and if there is no such stage, pay may be fixed at the next higher stage.

Illustration:

A person drawing emoluments as Basic Pay - Rs. 34,000/- and Dearness Allowance - Rs.44,200/- (DA @ 130%) with increment @ 3% per annum on the basic pay, is appointed in Central Govt. in the Level 11 of Pay Matrix (in 7th CPC) with DA @ 10% on deputation basis, his pay will be fixed as under:-

a. Adding one increment to the basic pay in the substantive post in parent cadre:

Pay in parent cadre post = Rs. 34,000/-.

Increment = 3% of Rs. 34,000/- = Rs. 1,020/-

Adding one increment = Rs. 35,020/- [i.e. Rs. 34,000/- + Rs. 1,020/-]

b. Pay and DA admissible in parent cadre:

DA @ 130% on basic pay = Rs. 45,526/- (130% of Rs. 35,020/-) Total emoluments in the parent cadre = Rs. 80,546/- (Rs. 35,020/- + Rs. 45,526/-)

c. Now, fixing pay in ex-cadre post in Level 11 of Pay Matrix (with DA @10%) on the basis of emoluments drawn in parent cadre:

Pay in ex-cadre i.e. Rs. 80,546/- shall comprise of Rs. 73,224/- (Basic Pay) + Rs. 7,322/-(DA @ 10%)

Pay Matrix

Band Pay	**15600-39100**
Grade Pay	**6600**
Level	11
3	71800
4	74000

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
about:blank
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

Since there is no cell in Level 11 of Pay Matrix matching Rs. 73,224/-pay will be fixed at Rs.74,000/- i.e. next cell in higher stage. So, the pay in ex-cadre post will be fixed at Rs.74,000/.

In case of reverse foreign service if the appointment is made to post whose pay structure and/or DA pattern is dissimilar to that in the parent organization, the option for electing to draw the basic pay in the parent cadre [along with the Deputation (Duty) Allowance thereon and the personal pay, if any] will not be available to such employee.

(ii) Deputation from State Government/UTs Administration to Central Government:

(a) When the Level (in Pay Matrix)/Pay Scale of the post in the parent cadre and that attached to ex-cadre post are based on the same index level and the DA pattern is also same, the pay may be fixed as provided under 5.1(i) above.

(b) If the appointment is made to a post whose pay structure and/or Dearness Allowance (DA) pattern is dissimilar to that in the parent organization, the pay may be fixed as provided under 5.1(ii) (b) above.

The basic pay from time to time after pay fixation should not exceed the maximum of the pay in the level of the ex-cadre post.

5.2 In cases of appointment from one ex-cadre post to another ex-cadre post where the employee opts to draw pay in the Level (in Pay Matrix)/Pay Scale of the ex-cadre post, the pay in the second or subsequent ex-cadre post should be fixed under the normal rules with reference to the pay in the cadre post only. However, in respect of appointments to ex-cadre posts carrying Level (in Pay Matrix)/Pay Scale identical to that of the ex-cadre post(s) held on an earlier occasion(s), it may be ensured that the pay drawn in subsequent appointment should not be less than the pay drawn earlier.

5.3 In cases of appointments to a second or subsequent ex-cadre post(s) in a higher Level (in Pay Matrix)/Pay Scale than that of the previous ex-cadre post, the pay may be fixed with reference to the pay drawn in the cadre post and if the pay so fixed happens to be less than the pay drawn in the previous ex-cadre post, the difference may be allowed as Personal Pay to be absorbed in future increases in pay. This is subject to the condition that on both the occasions, the employee should have opted to draw pay in the Level (in Pay Matrix)/Pay Scale attached to the ex-cadre posts.

Note-1: The term parent post and basic pay means the post held on regular basis in the parent organisation and pay drawn/ admissible in such a post respectively.

Note-2: An officer who may be holding a higher post on ad-hoc basis in the cadre at the time of proceeding on deputation/foreign service would be considered to have vacated the post held on ad-hoc basis and proceeded on deputation/foreign service from his/her regular post. During the period of deputation/foreign service, he/she shall earn notional increments in the parent cadre post. On reversion, if he/she is re-appointed to the higher post on regular or ad-hoc basis his pay will get fixed with reference to the pay admissible in the lower post on the date of such re-appointment. In such cases, if his/her pay gets fixed at a stage lower than that of his junior(s) who continued to serve in the cadre, no stepping up will be admissible

less than the pay drawn earlier while holding the post on ad-hoc basis the pay earlier drawn will be protected. Therefore, those Central Government employees who are already holding a higher post on ad-hoc basis or expecting it shortly in the parent cadre may weigh all relevant considerations before opting for deputation/foreign service. This note of caution will be applicable to employees of other organizations wishing to apply for posts on deputation in Central Government, if governed by similar rules in parent organization.

Note-3: Pay of an officer appointed on deputation/foreign service on ad hoc basis pending selection of a regular incumbent may also be regulated in accordance with provisions of Paras 5.1 & 6.1 of this O.M.

Note-4: The provisions of this Para as well as Para 6 will not apply to appointments on Personal Staff of Ministers. Such appointments will be regulated by separate specific orders issued by the Government in that behalf.

[Para 5 of DoPT's OM No. 6/8/2009-Estt.(Pay-II) dated 17.06.2010 read with OM No. 2/10/2018-Estt. (Pay-II) dated 2.3.2021]

DEPUTATION (DUTY) ALLOWANCE

6.1 The Deputation (Duty) Allowance admissible shall be at the following rates:

(a) Within the same station, the allowance will be payable at the rate of 5% of basic pay subject to a maximum of Rs. 4500/- p.m.;

(b) In case of change of station, the allowance will be payable at the rate of 10% of basic pay subject to a maximum of Rs. 9000/- p.m.;

(c) The ceilings will further rise by 25 percent each time Dearness Allowance increases by 50 percent; and

(d) Basic Pay, from time to time, plus Deputation (Duty) Allowance shall not exceed the basic pay in the Apex level i.e. Rs. 2,25,000/-. In the case of Government servants receiving Non-Practicing Allowance, their basic pay plus Non-Practicing Allowance plus Deputation (Duty) Allowance shall not exceed the average of basic pay of the revised scale applicable to the Apex Level and the Level of the Cabinet Secretary i.e. Rs. 2,37,500/-.

6.1.2 In cases where the basic pay in parent cadre has been upgraded (upto Level 13 A) on account of Non-Functional Upgradation (NFU), Modified Assured Career Progression Scheme (MACP), Non-Functional Selection Grade (NFSG) etc., and the officer has opted for such upgraded pay of the parent cadre, in that event, the upgraded basic pay under such upgradations shall not be taken into account for the purpose of Deputation (Duty) Allowance. In such cases, the Deputation (Duty) Allowance will be calculated taking the basic pay of the parent cadre which the officer was getting before such upgradation and the amount of the same would be further regulated every year on the basis of the pay arrived at by giving annual increments on the presumptive pay.

6.1.3 However, if the upgradation is to Level 14 (in the Pay Matrix) or above, he shall be given the option to draw the upgraded basic pay under such upgradations without Deputation (Duty) Allowance or the pay which he was drawing before such upgradation with Deputation (Duty) Allowance, whichever is more beneficial as per the option of the officer.

6.1.4 In the case of Proforma Promotion under Next Below Rule (NBR), if such a Proforma Promotion (upto Level 13 A) is in a Level of the Pay Matrix which is higher than that of the ex-cadre post, and the officer has opted for the upgraded pay of the Proforma Promotion, the basic pay under such Proforma Promotion shall not be taken into account for the purpose of Deputation (Duty) Allowance. Deputation (Duty) Allowance will be calculated taking into account the basic pay which the officer was getting before such Proforma Promotion. The amount of Deputation (Duty) Allowance would be calculated on the basis of the pre-upgraded presumptive pay that the officer was drawing prior to Proforma Promotion and the amount of the same would be further regulated every year on the basis of the pay arrived at by giving annual increments on the presumptive pay.

6.1.5 However, if such a Proforma Promotion under NBR is in a Level of the pay matrix which is equal to or below that of the ex-cadre post, Deputation (Duty) Allowance shall be admissible on the basic pay of the parent cadre post allowed under the Proforma Promotion, if opted by the deputationist.

6.1.6 However, if the upgradation is to Level 14 or above of the Pay Matrix, he shall be given the option to draw the upgraded basic pay under such Proforma Promotion without Deputation (Duty) Allowance or the pay which he was drawing before grant of Proforma Promotion with Deputation (Duty) Allowance, whichever is more beneficial as per the option of the officer. The amount of Deputation (Duty) Allowance would be calculated on the basis of pre-upgraded presumptive pay that the officer was drawing prior to the grant of Proforma Promotion and the amount of the same would be further regulated every year on the basis of the pay arrived at by giving annual increments on the presumptive pay.

[DoPT's OM No. 2/11/2017-Estt.(Pay-II) dated 24.11.2017 and DoPT's OM No. 2/11/2017-Estt.(Pay-II) dated 15.3.2021]

Note: Basic Pay in the revised pay structure (the pay structure based on 7th CPC recommendations) means the pay drawn by the deputationist, from time to time, in the prescribed Level (in Pay Matrix) of the post held by him substantively in the parent cadre, but does not include any other type of pay like personal pay, etc.

Note: 1 The term 'same station' for the purpose will be determined with reference to the station where the person was on duty before proceeding on deputation.

Note: 2 Where there is no change in the headquarters with reference to the last post held, the transfer should be treated as within the same station and when there is change in headquarters it would be treated as not in the same station. So far as places falling within the same urban agglomeration of the old headquarters are concerned, they would be treated as transfer within the same station.

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
about:blank
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

particular area on account of the condition of living there being particularly arduous or unattractive. Where special rate is more favourable than that given in Para 6.1 above, employees deputed to the area will be given the benefit of the special rate.

6.3.1 If an employee with the permission of the competent authority, proceeds on deputation/foreign service from one ex-cadre post to another ex-cadre post in the same or another organization without reverting to his parent cadre, and if the second ex-cadre post is at the same station as the first one, the rate of Deputation (Duty) Allowance would remain unchanged.

6.3.2 In cases where a person on deputation/foreign service is transferred by the borrowing authority from one station to another without any change in the post held by him. The rate of Deputation (Duty) Allowance will be refixed as per 6.1 (b).

[Para 6.2 and 6.3 of DoPT's OM No. 6/8/2009-Estt.(Pay-II) dated 17.06.2010]

ADMISSIBILITY OF PAY, ALLOWANCES AND BENEFITS WHILE ON DEPUTATION/FOREIGN SERVICE

7.1 Any project allowance admissible in a project area in the borrowing organization may be drawn in addition to Deputation (Duty) Allowance.

7.2 Any special allowance granted to an employee in the parent Department under FR 9(25) or a corresponding rule of parent organization should not be allowed in addition to Deputation (Duty) Allowance. However, the borrowing department may allow in addition to Deputation (Duty) Allowance, under special circumstances, any special allowance attached to the post held by the employee in his/her parent Department, by suitably restricting the Deputation (Duty) Allowance. This will require the specific and prior approval of Department of Personnel &Training.

7.3 In case special allowance is attached to the scale of pay of the ex-cadre post and the employee has opted to draw pay in that scale, then, in addition to the pay in that scale, he will also be entitled to draw such special allowance. However, such special allowance will not be admissible if he has opted to draw pay in the parent cadre scale/grade pay plus Deputation (Duty) Allowance.

7.4 Personal pay, if any, drawn by an employee in his parent department will continue to be admissible on deputation/foreign service if he/she opts to draw pay in the parent cadre plus Deputation (Duty) Allowance. No Deputation (Duty) Allowance on this personal pay will, however, be admissible.

7.5 **Increments** - The employee will draw increment in the parent cadre or in the Level (in the Pay Matrix) attached to the deputation post as the case may be, depending on whether he has opted for the parent cadre pay plus Deputation (Duty) Allowance or the pay of the deputation post. If he has opted for pay of the deputation post, notional increments shall also continue to accrue to him in the post held on regular basis in the parent cadre/organization for the purpose of regulation of pay on repatriation to the parent cadre/post at the end of the tenure.

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm
File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
about:blank
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

7.6(a) Such allowances as are not admissible to regular employees of corresponding status in the borrowing organisation shall not be admissible to the officer on deputation/ foreign service, even if they were admissible in the parent organisation.

(b) Following allowances will be regulated with mutual consent of the lending and borrowing organization:

a. HRA/Transport Allowance.

b. Joining time and Joining Time Pay.

c. Travelling Allowances and Transfer T.A.

d. Children Education Allowance.

e. LTC.

(c) Following allowances/facilities will be regulated in accordance with the rules as explained against each:

i. **Dearness Allowance** - The employee shall be entitled to dearness allowance at the rates prevailing in the borrowing organization or in the lending organization depending on whether he has opted to draw pay of the ex-cadre post or the parent cadre post.

ii. **Medical Facilities** - This will be regulated in accordance with the rules of the borrowing organization.

iii. **Leave** - An officer on deputation/foreign service shall be regulated by the Leave Rules of the parent organization. If, however, an employee proceeds from vacation department to non-vacation department, or vice-versa, he shall be governed by Leave Rules of the borrowing organization. At the time of reversion from the deputation post to the parent cadre, the borrowing organization may allow him/her leave not exceeding two months. The employee should apply for further leave to his Cadre Controlling Authority.

[Para 7.1-7.6 of DoPT's OM No. 6/8/2009-Estt. (Pay-II) dated 17.06.2010]

(d) **Military Service Pay (MSP)**: In case an army officer entitled to Military Service Pay in parent cadre opts for parent cadre pay on deputation to a civil post, MSP will be admissible as a separate element, provided Deputation (Duty) Allowance will not be reckoned on MSP but only on Basic Pay.

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 01:07 pm

[On the basis of clarification dated 16.2.2017 issued by D/o Expenditure]

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
about:blank
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

7.7 Leave Salary/Pension/NPS Contribution

i. As at present, allocation of leave salary and pension contribution between different Ministries/Departments of Central Government and between Central and State Government has been dispensed with. In such cases of deputation from Central Government to State Government and vice-versa, liability for bearing leave salary vests with the Department from which the officer proceeds on leave or which sanctioned leave and no contributions are payable to the lending organization. Liability for pension/employee's contribution to CPF will be borne by the parent department, to which the officer permanently belongs at the time of retirement and no proportionate contribution will be recovered.

ii. In case of deputation of Central Government employees on foreign service terms to Central Public Sector Undertakings/ State Public Sector Undertakings and Autonomous Bodies etc., leave salary contribution (except for the period of leave availed of on foreign service) and pension contribution/ Contributory Provident Fund (CPF) (Employer's share) contribution are required to be paid either by the employee himself or by the borrowing organization to the Central Government. In cases of reverse deputation from Central Public Sector Undertakings/ State Public Sector Undertakings/ Autonomous Bodies/local bodies to Central Government, the employer's share of CPF for the period of deputation to the Central Government will be borne either by the employee himself or borrowing organisation i.e. Central Government depending on the terms of deputation. A clear mention of the stipulation on whether the Central Government or the employee would bear the liability may be made in the terms of deputation.

[DoPT's OM No. 6/8/2009-Estt.(Pay-II) dated 15.2.2012]

iii. In cases of reverse deputation from Central Public Sector Undertakings/ State Public Sector Undertakings/ Autonomous Bodies/local bodies to Central Government, the question regarding leave salary and pension contribution will be decided by mutual consent.

iv. In case of employees covered under New Pension Scheme (NPS), the borrowing department shall make requisite contribution to the NPS account of the employee.

TENURE OF DEPUTATION/FOREIGN SERVICE

8.1 The period of deputation/ foreign service shall be as per the provisions of the RRs of the ex-cadre post or 5 years in case no tenure regulations exist for the ex-cadre post.

8.2 In case where the period of deputation/foreign service prescribed in the RRs of the ex-cadre post is 5 years or less than 5 years, the borrowing Ministry/Department/ Organization may grant extension upto the 6th year after obtaining orders of their Secretary (in the Central Government)/ Chief Secretary (in the State Government)/ equivalent officer (in respect of other cases) and for the 7th year with the approval of the Minister of the borrowing Ministry /Department and in respect of other organizations with the approval of the Minister of the borrowing Ministry/Department with which they are administratively concerned.

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm
16
File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
about:blank
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

8.3.1 The borrowing Ministries/Departments/Organizations may extend the period of deputation up to the seventh year where necessary in public interest, subject to the following conditions:

i. The extension would be subject to the prior approval of the lending organization, the consent of the official concerned and wherever necessary, the approval of the UPSC/ State Public Service Commission and Appointment Committee of Cabinet (ACC).

ii. If the borrowing Ministry/Department/Organization wishes to retain an officer beyond the prescribed tenure, it shall initiate action for seeking concurrence of lending organization, individual concerned etc. six months before the date of expiry of tenure. In no case it should retain an official beyond the sanctioned term unless prior approval of the competent authority to grant further extension has been obtained.

iii. No further extension beyond 7th year shall be granted.

8.3.2 Admissibility of Deputation (Duty) Allowance would be only upto fifth year.

[DoPT's OM No. 2/6/2016-Estt.(Pay-II) dated 23.02.2017]

COOLING OFF

9.1 There shall be a mandatory 'cooling off' period of three years after every period of deputation/foreign service up to Joint Secretary level posts (i.e. deputation post carrying pay in Level-14 of the Pay Matrix) and one year for Additional Secretary level posts (i.e. deputation post carrying pay in Level-15 of the Pay Matrix).

The Ministries/Departments may not sponsor name of any such officer who is not likely to complete the mandatory 'cooling off' period by the time the officer is likely to be selected. Further, while sponsoring the name of any such officer who has not completed the mandatory cooling off period, the parent cadre authority may inform the borrowing department that the officer will be relieved only after he/she completes the mandatory cooling off period.

[DoPT's OM No. 2/1/2012-Estt.(Pay-II) dated 4.1.2013]

9.2 A Central Government employee shall be eligible for deputation/foreign service to posts in State Government/State Government Organization/ UT Administration / Government of UT's Organization/Autonomous Bodies. Trusts, Societies, PSUs etc. not controlled by the Central Government only after he has completed 9 years of service and is clear from the vigilance angle.

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm
File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
about:blank
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

9.2.1 However, with the approval of the Minister-in-charge of the Ministry/Department/ Organization:

i. Central Government employee after completion of 7 years of service in his/her cadre, may be allowed to go on deputation to any State of North-Eastern Region and Union Territories of Jammu & Kashmir, Ladakh, Andaman & Nicobar and Lakshadweep or on foreign service to any entity controlled by and located in the afore said States/ Union Territories;

ii. Central Government employees may be allowed to go on deputation to State Governments /Union Territories or on foreign service to any entity controlled by and located in the States/ Union Territories on spouse ground after completion of 6 years of service in the cadre.

[DoPT's OM No. 2/15/2017-Estt.(Pay-II) dated 18.10.2018]

10. If during the period of deputation/foreign service, on account of Proforma Promotion in the parent cadre the official concerned becomes entitled to a higher pay in the Level (in the Pay Matrix) in the parent cadre *vis-a-vis* that of the ex-cadre post, the official shall complete his/her normal /extended tenure of deputation already sanctioned with the approval of the competent authority. The pay shall be regulated as under:

a. If the Level (in the Pay Matrix) of the officer in the parent cadre becomes higher than that of the deputation post after getting Proforma Promotion, he may be allowed the pay in the Level (in the Pay Matrix) of the post to which he is promoted, if he so opts. In such cases, extensions in deputation after employee has received the Proforma Promotion may be considered as per the instruction in paras 8.1 to 8.3.2.

b. If he draws the pay in the Level (in the Pay Matrix) attached to the deputation post, on reversion to his parent cadre, his pay may be fixed by allowing him notional increments in his regular post in the parent department.

c. If the Level (in the Pay Matrix) of the officer in the parent cadre becomes higher than that of the deputation post on getting financial upgradation under the ACP/MACP scheme, the officer may be allowed to draw the pay in Level (in the Pay Matrix) to which he becomes entitled to under the ACP/MACPS, if opted for by him, as laid down in Para 27 of Annexure I to the DoPT OM No. 35034/3/2008 -Estt.(D) dated 19th May, 2009.

[DoPT OM No. 35034/3/2008 -Estt.(D) dated 19th May, 2009]

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm

PREMATURE REVERSION OF DEPUTATIONIST TO PARENT CADRE.

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
about:blank
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

11. Normally, when an employee is appointed on deputation/foreign service, his services are placed at the disposal of the parent Ministry/ Department/Organization at the end of the tenure. However, as and when a situation arises for premature reversion to the parent cadre of the deputationist, his services could be so returned after giving a notice of at least three months to the lending Ministry/Department/ Organization and the employee concerned.

OVERSTAY ON DEPUTATION

12. The deputationist officer is deemed to have been relieved on the date of expiry of the deputation period unless the competent authority has with requisite approvals, extended the period of deputation, in writing, prior to the date of its expiry. It will be the responsibility of the immediate superior officer to ensure that the deputationist does not overstay. In the event of the officer overstaying for any reason whatsoever, he/she is liable to disciplinary action and other adverse Civil/Service consequences which would include the period of unauthorized overstay not being counted for service for the purpose of pension and that any increment due during the period of unauthorized overstay being deferred with cumulative effect, till the date on which the officer rejoins his parent cadre.

[DoPT's OM No. 6/8/2009-Estt.(Pay-II) dated 1.3.2011]

All the Ministries/Departments are to ensure that deputations are strictly monitored by the lending Government Ministry/Department/Organization. Requests of the borrowing authorities for no objection to extension of deputation should be closely scrutinized to curb tendency to allow extensions on extraneous ground and overstay.

[DoPT's OM No. 6/8/2009-Estt.(Pay-II) dated 16.5.2013]

RELAXATION OF CONDITIONS

13. Any relaxation of these terms and conditions will require the prior concurrence of the Department of Personnel & training.

DATE OF EFFECT

14. These orders will take effect from 1.1.2016 and shall be applicable to all officers who were on deputation on 1.1.2016 or appointed thereafter except for the following:

i. Revised rates of Deputation (Duty) Allowance shall be applicable from 1.7.2017.

ii. Provisions of Para 8.1 and 8.2 shall be applicable from 18.05.2018. iii. Provisions of Para 8.3.1(iii) shall be applicable from 17.02.2016. iv. Provisions of Para 9.2.1 shall be applicable from 18.10.2018.

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
about:blank
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

3(b)(iv) of this OM, shall take effect from the date of issue of the OM i.e. 15.03.2024.

15. List of the OMs mentioned in this document is annexed. In case, any reference to the relevant OM is required, the same may be accessed from DoPT's website.

ANNEXURE

List of OMs mentioned in this Document

S. No.	O.M. No.	O.M. Date	Subject
1.	6/8/2009- Estt.(Pay-II)	01.03.2011	Overstay while on deputation.
2.	6/8/2009- Estt.(Pay-II)	15.02.2012	Clarification regarding regulation of payment of employer's share of contribution to the Contributory Provident Fund during the period of reserve deputation.
3.	6/5/2012- Estt.(Pay-II)	30.11.2012	Provisions relating to proforma promotion.
4.	2/1/2012- Estt.(Pay-II)	04.01.2013	Sponsoring of names of officers for deputation.
5.	6/8/2009- Estt.(Pay-II)	16.05.2013	Proper Monitoring of deputation by the lending departments.
6.	2/6/2016- Estt.(Pay-II)	17.02.2016	Delegation of powers to Ministries / Departments/Borrowing Organizations to extent deputation tenure upto 7 years in cases of Deputation covered by DOPT's OM No. 6/8/2009-Estt.(Pay-II) dated 17th June, 2010 – regarding.
7.	2/6/2016- Estt.(Pay-II)	23.02.2017	Admissibility of Deputation (Duty) Allowance while on deputation – regarding.
8.	2/11/2017- Estt.(Pay-II)	24.11.2017	Grant of Deputation (Duty) Allowance – Recommendations of the Seventh Central Pay Commission – regarding.
9.	2/6/2018- Estt.(Pay-II)	18.05.2018	Amendment in Para 8.1 and Para 8.2 of deputation guidelines issued vide OM No.6/8/2009-Estt.(Pay-II) dated 17th June, 2010.
10.	2/15/2017- Estt.(Pay-II)	18.10.2018	Transfer of deputation/ foreign service of Central government Employees to ex-cadre posts under the State Governments/ Union Territories or to any entity controlled by and located in the States/UTs – relaxation of para 8.5 of O.M. dated 17.06.2010.

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
about:blank
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

			guidelines on deputation issued vide OM No. 6/8/2009-Estt.(Pay-II) dated 17.06.2010 according to 7th CPC pay structure.
12.	2/11/2017- Estt.(Pay-II)	15.03.2021	Grant of Deputation (Duty) Allowance in cases where the basic pay in parent cadre has been upgraded on account of NFU, MACP, NFSG, etc. in the 7 th CPC context – clarification.
13.	2/9/2018- Estt.(Pay-II)	12.04.2021	Amendment in Para 3.4 of deputation guidelines issued vide OM No.6/8/2009-Estt.(Pay-II) dated 17th June, 2010.
14.	AB.14017/24/2022-Estt.(RR)	31.08.2022	Consolidated and revised instructions on constitution of Search Committees and Search-cum-Selection Committees
15.	40/1/2022-EO(CVO)	18.11.2022	Guidelines/procedure for appointment of CVOs in CPSEs and other organizations under Central Government and their service conditions.
16.	1705650752584	19.01.2024	Consolidated instructions governing Central Staffing Scheme (CSS).
17.	*OM No.6/8/2023-Pers.Policy (Deputation/Re-employment) Pt.XV*	15.03.2024	Instructions governing appointment and terms and conditions of deputation of Group 'A' officers of the Central Government to ex-cadre posts under a State Government/UT Administration including PSUs/ Autonomous bodies/Statutory Bodies/ Universities/ Local Bodies under the States/UT Administration in partial modification of the instructions governing deputation/foreign service and para 1.3 of this Department's OM No.AB-14017/2/2007-Estt(RR) dated 29.02.2008

(Sign of Authority)

Mahesh Kumar

Under Secretary

23040489

Frequently Asked Questions

Q.1 Applicability of OM dated 15.03.2024?

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

Ans. Cases involving deputation of Group 'A' officers of the Central Government to ex-cadre posts under a State Government/UT Administration including PSUs/ Autonomous bodies/Statutory Bodies/ Universities/Local Bodies under the States/UT Administration.

Q.2 Whether applicable to cases involving deputation of Central Govt. officers of Pay level-14 and above who wish to apply for deputation to posts under Central Govt.?

Ans. No. Their deputation shall continue to be governed by the existing deputation guidelines issued vide DoPT's OM No. 6/8/2009-Estt. (Pay II) dated 17.06.2010, as amended from time to time.

Q3. An officer in Pay Level 13 while on deputation, gets promoted to Pay Level-14 in his parent cadre. In such a situation can the officer continue his deputation or he/she needs to report back to his/her parent cadre?

Ans. The officer who gets promoted to Pay Level 14 in the parent Cadre while on deputation may be allowed to complete already approved deputation tenure.

Q4. What is the total allowable period of deputation in cases governed by the provisions of DoPT's OM dated 15.03.2024?

Ans. Total allowable period of deputation to the posts under State govt. /UT Administration including PSUs/ Autonomous bodies/Statutory Bodies/Universities/Local Bodies under the States/UT Administration would be restricted to 5 years in entire career.

Q5. Who is the Authority competent to send such proposal to obtain requisite approvals as prescribed in DoPT's OM dated 15.03.2024 or any relaxation to the provisions thereof, where admissible?

Ans. The proposal should be sent by the Cadre Controlling Authority of the officer concerned with the approval of the Minister in-charge of the administrative ministry/department along with the NOC of the borrowing State/UT government.

Q6. What would happen if the officer does not repatriate to parent cadre in anticipation of extension?

Ans. In the event the officer overstays for any reason whatsoever without formal approval of the Competent Authority to the extension sought, he/she is liable for disciplinary action and other adverse Civil/ Service consequences which would include the period of overstay not being counted towards service for the

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 09:07 am

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
about:blank
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

effect, till the date on which the officer re-joins in his parent Cadre.

Q8. Are the provisions of the OM dated 15.03.2024 applicable to group A officers of the State government?

Ans. No.

Q9. Does the deputation period spent in Group B will also count towards the total deputation tenure availed by an officer of central government in state government /UT Administration including PSUs/ Autonomous bodies/Statutory Bodies/Universities/Local Bodies under the States/UT Administration?

Ans. No. Provisions of DoPT's OM dated 15.03.2024 are applicable to only the cases involving deputation of Group A officers of the Central Government.

Q.10 Documents required to be submitted while sending proposal to DoPT for consideration in terms OM dated 15.03.2024.

Ans. Checklist for submitting the proposal to DoPT is mentioned below:

1.	Proposal Text		
2.	Name /Service /Cadre /Batch of the Officer		
3.	Updated Executive Record Sheet/Service profile of the officer	☐ Attached ☐ NA	(Annexure- I)
4.	Home State of the Officer		
5(a).	Vigilance status of the officer	☐ Attached ☐ NA	(Annexure- II)
5(b).	Date of filing of Annual IPR as filed in the month of January this year or otherwise by the officer	Date: 26	

	representation/ consent of the officer		
7.	NOC from the Concerned State Governments/CCAs(Cadre Controlling Authority):		
(a)	State Governments/CCA-1	Parent/ Accepting Cadre: State Govt of XYZ ☐ Attached☐ NA	(Annexure- IV)
(b)	State Governments/CCA-2	Parent/ Accepting cadre: State Govt of ABC ☐ Attached☐ NA	(Annexure- V)
(c)	State Governments/CCA-3	Parent /Accepting cadre: State Govt of PQR ☐ Attached☐ NA	(Annexure- VI)
9.	Details of Cadre Strength/ In-Position strength of the Service as on first January of the year as per Civil List	☐ Attached☐ NA	(Annexure- VII)
10(a).	Draft ACC Note	☐ Attached☐ NA	(Annexure-VIII)
10(b).	Point for consideration of ACC	-	-
11.	Relevant Rules/ Policy	☐ Attached☐ NA	(Annexure-IX)
12.	Details, if the proposal involves relaxation of the policy	-	
13.	Administrative/ functional justification of the proposal.	-	-
14.	Approval of the Minister-in-charge in Self contained Note	☐ Attached☐ NA	(Annexure-X)
15.	9 years of Service in Group 'A'	-	-
16.	Details of the Cadre Clearance	-	-
17.	Pay level of the Officer	-	-
18.	Details of deputation to State/UTsGovernments etc. as indicated in para 3 of DoPT's OM dated 15.03.2024may be provided	-	-
19.	Period of deputation for which approval is sought	-	-

Signature: _____

Name: _____

Designation:(Joint Secretary or equivalent or above)

Stamp/Seal: _____

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
about:blank
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

Ans. References seeking approval of the designated Committee to the proposal before it is submitted for approval by the Appointments Committee of the Cabinet (ACC) should be made only on e-file, with details/ self-contained notes, strictly in accordance with the procedure laid down in this Department's O.M. No. 43011/9/2014-Estt.D dated 28th October, 2015 and Secretary (P), DoPT's DO letter No. I-28029/30/2021-Coord dated 12.09.2022

(Sign of Authority)
Mahesh Kumar
Under Secretary
23040489

******

File No. Z-28015/122/2025-PMSSY-IV (Computer No. 8343520)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 19/09/2025 01:07 pm

File No. Z-28015/88/2025-PMSSY-IV (Computer No. 8335252)
Generated from eOffice by VAISHALI VINAYAK, SO(VV)-PMSSY-IV, SECTION OFFICER, DOHFW DEPARTMENT on 15/05/2025 11:53 am

about:blank

DDA AIIMS PATNA <dda@aiimspatna.org>

Extension of (a) Transport Allowance at double the normal rates to Persons with Disabilities in accordance with Department of Expenditure's OM dated 15.09.2022 and (b) Special Allowance for Child Care for Women with Disabilities in accordance with DoPT's instructions dated 16.08.2017.

pmssysection iv <pmssysectioniv@gmail.com> Mon, Nov 17, 2025 at 10:42 AM
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, madhabananda@gmail.com, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, drppjoshi@aiimsnagpur.edu.in, Executive Director Raebareli <edaiimsrbl@gmail.com>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, "Prof. Dr. D.K. Singh, Director" <director@aiimsbathinda.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, "Dr.Shakti kumar Gupta" <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, ed@aiimsrajkot.edu.in, edaiimsrajkot2020@gmail.com, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, sachimohanty@rediffmail.in, "Sharma, DN" <sharmadn@aiims.edu>
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, "Dy Director Administration AIIMS, Raebareli" <ddaaiimsrbl@gmail.com>, "Dr. Pradip Kumar" <kpradip10@gmail.com>, dda@aiimskalyani.edu.in, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, dda@aiimsbilaspur.edu.in, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, aps101982@rediffmail.com, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, dda@aiimsguwahati.ac.in, raj08642@gmail.com, Mukesh Kumar <mac.prasad@gmail.com>, ddaaiimsawantipora1@gmail.com, neelam.chachra@nic.in, ":" <Ak.biswas57@nic.in>, premprakash.bth@gov.in, manoj@ndma.gov.in, Vaishali Vinayak <vaishali.vinayak@gov.in>, Devender DKumarGothal <dev.gothal@gov.in>, r.ahul@gov.in, Suprava Poddar <sup15.81997@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officers of PMSSY-IV Section at - ak.biswas57@nic.in; premprakas h.bth@gov.in; dev.gothal@gov.in; vaishali.vinayak@gov.in; manoj@ndma.gov.in; r.ahul@gov.in; sup15.81997@gov.in;

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

3 attachments

Letter (241).pdf
92K

15.09.2022.pdf
285K

16.08.2017.pdf
56K

Z-28015/7/2025-PMSSY-IV
8314093
Government of India
Ministry of Health & Family Welfare
PMSSY-IV Section

Nirman Bhawan, New Delhi
Dated 18.07.2025

To,

Executive Director of all new AIIMS

Subject: Extension of (a) Transport Allowance at double the normal rates to Persons with Disabilities in accordance with Department of Expenditure's OM dated 15.09.2022 and (b) Special Allowance for Child Care for Women with Disabilities in accordance with DoPT's instructions dated 16.08.2017.

Madam/Sir,

I am directed to refer to the subject cited above and to covey the approval of competent authority for extending the following allowances to all eligible employees of AIIMS Institutions with immediate effect:

(a) Transport Allowance at double the normal rates to Persons with Disabilities in accordance with Department of Expenditure's OM dated 15.09.2022.

(b) Special Allowance for Child Care for Women with Disabilities in accordance with DoPT's instructions dated 16.08.2017

2 The expenditure on this account will be met from the overall budget allocated to the Institutes under GIA (Salary) head of the PMSSY Scheme.

3 This issues with the concurrence of IFD vide CD No. 1221 dated: 16/07/2025.

Digitally signed by ARUN KUMAR BISWAS
Date: 23-07-2025 12:27:51

Yours faithfully

(Arun Kumar Biswas)
Under Secretary to the Government of India
Tel:011-23061343
ak.biswas57@nic.in

Copy to:-

1. Deputy Director (Administration), of all new AIIMS
2. Under Secretary (INI-I), MoHFW, New Delhi.

No.21/1/2018-E.IIB
Government of India
Ministry of Finance
Department of Expenditure
***

North Block, New Delhi.
Dated the 15th September, 2022.

OFFICE MEMORANDUM

Subject: Compendium of Instructions regarding grant of Transport Allowance at double the normal rates to persons with disabilities employed in Central Government-regarding

The Department of Expenditure, Ministry of Finance has issued various instructions from time to time regarding grant of Transport Allowance at double the normal rates to persons with disabilities employed in Central Government. Such instructions were issued a long back. Therefore, the existing instructions have been reviewed and in supersession of all earlier instructions issued on the subject, a consolidated Master O.M. is hereby circulated for compliance by all Ministries/ Departments.

2. This is issued with the approval of Finance Minister.

(Nirmala Dev)
Director

To,

All Ministries and Departments of the Govt. of India as per standard distribution list.

Copy to: C&AG and U.P.S.C. etc. as per standard endorsement list.

File No. Z-28015/7/2025-PMSSY-IV (Computer No. 8314093)
Generated from eOffice by SANKAR GARG, SO(SG)-PMSSY-IV-MOHFW, SECTION OFFICER, DOHFW DEPARTMENT on 18/07/2025 04:36 pm

MINISTRY OF FINANCE
DEPARTMENT OF EXPENDITURE
****

COMPENDIUM

ON

Instructions regarding Grant of Transport Allowance at double the normal rates to persons with disabilities employed in Central Government.

****

CONTENTS

S.No.	Particulars	
A.	Scope of application	
B.	Revised and Updated Provisions	
	1.	Categories of disabilities for the purpose of grant of Transport Allowance at double the normal rates
	2.	Criteria for percentage of disability
	3.	Procedure to be followed for grant of Transport Allowance at double the normal rates.
	4.	Rates of Transport Allowance.
	5.	Conditions for grant of Transport Allowance at double the normal rates.
	6.	Admissibility of Transport Allowance at double the normal rate during different circumstances.
C.	7.	Appendix - Earlier orders on Transport Allowance at double the normal rates to persons with disabilities

A. Scope of Application:

These instructions will apply to Central Government civilian employees with Benchmark Disabilities mentioned in Para (B) (1). The instructions will also apply to the civilian employees with Benchmark Disabilities paid from the Defence Service Estimates. In respect of the Railway employees, separate orders will be issued by the Ministry of Railways.

B. Revised and updated provisions

The consolidated and updated provisions on various aspects on grant of Transport Allowance at double the normal rates to persons with Benchmark disabilities employed in Central Government, are as under:-

1. Categories of disabilities for the purpose of grant of Transport Allowance at double the normal rates:

1.1. The Central Government employees with following categories of disabilities as mentioned in Rights of Persons with Disabilities (RPwD) Act 2016 of D/o Empowerment of Persons with Disabilities (EPwD), shall be paid Transport Allowance at double the normal rates subject to fulfilment of the stipulated conditions:

Sl. No.	Name of Disability
i.	**Blindness**
ii.	**Locomotor disability including Cerebral Palsy, Leprosy cured, Dwarfism, Acid Attack victims, Muscular Dystrophy and Spinal Deformity etc.**
iii.	**Deaf & Dumb and hearing impairment**
iv.	**Autism Spectrum disorder, Intellectual disability**
v.	**Chronic Neurological conditions** **(a) Multiple Sclerosis** **(b) Parkinson's disease**
vi.	**Blood Disorder:** **(a) Haemophilia** **(b) Thalassemia** **(c)Sickle Cell disease**
vii.	**Multiple disabilities from amongst persons under clauses (i) to (vi)**

2.. Eligibility Criteria:

2.1. Employees with Benchmark disability having valid certificate of disability shall be eligible to draw Transport Allowance at double the normal rates.

2.2. Persons with Benchmark disability has been defined under Section 2 (r) of the RPwD Act, 2016.

-3-

3. Procedure to be followed for grant of Transport Allowance at double the normal rates:

3.1 The condition of recommendation of the concerned Head of Department of the Government Hospital, is **done away with** in terms of guidelines notified by D/o EPwD vide Notification dated 04.01.2018, as modified from time to time. The Certificate of Disability issued by the Certified Medical Authority may suffice. Employees covered under the preceding Para B (1) (i) to (vii) above shall apply for grant of Transport Allowance at double the normal rates to the Administrative authority of their Departments on the basis of Certificate of Disability issued by the Certified Medical Authority in terms of guidelines for the purpose of assessing the extent of specified disability notified on 04.01.2018 by D/o EPwD. In case of any doubt, the case may be referred to the concerned Head of Department of Government Hospital. The allowance may be granted with effect from the date, the Certificate of disability is received by the Administrative authority in the concerned Ministry/Department.

3.2. In case of doubt over Certificate of disability, the Head of the Department may refer the employee to the Government Civil Hospitals/Medical Authority for getting confirmation regarding disability. The employee may be reimbursed the actual travelling expenses subject to a maximum Travelling Allowance admissible for a journey on tour without any Daily Allowance for the period of journey and for halts. The period spent on journeys and also at the hospitals shall, however, be treated as duty. If any fee is charged by the Central Govt. Hospital/Union Territory Hospital/ State Government Hospitals, it shall be reimbursed to the employees concerned.

3.3. Government employee who at the time of appointment submit valid Disability Certificate issued by Certified Medical Authority in terms of Notification issued by D/o EPwD dated 04.01.2018 as amended from time to time, would be granted Transport Allowance at double the normal rates from the date of appointment itself. In all other cases, the Transport Allowance at double the rates would be admissible from the date, the requisite certificate is received by the Administrative authority concerned.

3.4. Government employees already getting the benefit of Transport Allowance at double the normal rate on the basis of certificates obtained from Government Civil Hospitals as per earlier instructions, would continue to get it on the basis of those certificates.

4. Rates of Transport Allowance:

4.1. The rates of Transport Allowance had been revised vide this Department's O.M. No. dated 7th July 2017 as per recommendations of 7th Central Pay Commission. The following rates of Transport Allowance are admissible to Central Government employees w.e.f. 01.07.2017:

-4-

Employees drawing pay in Pay Level:	Rates of Transport Allowance per month	
	Employees posted in the Cities as per Annexure-I.	Employees posted at all Other Places
9 and above	Rs. 7200 + DA thereon	Rs.3600+ DA thereon
3 to 8 and those drawing Pay of Rs. 24200/- and above in Level 1 & 2 of the Pay Matrix.	Rs. 3600 + DA thereon	Rs.1800+ DA thereon
1 and 2	Rs.1350 + DA thereon	Rs.900 + DA thereon

4.2. Persons with Benchmark Disabilities prescribed in Para B(1) above, shall be eligible for Transport Allowance at double the above rates.

5. Conditions for grant of Transport Allowance at double the normal rates:

Transport Allowance at double the normal rates shall be admissible subject to the following conditions:

5.1. The allowance shall not be admissible to those employees who have been provided with the facility of Government vehicle.

5.2. In respect of those employees who opt to continue in their pre-revised pay-Structure/pay scales, the corresponding Level in the Pay Matrix of the post occupied on 01.01.2016 as indicated in CCS (Revised Pay) Rules, 2016 would determine the allowance under these orders.

5.3. For Level 14 and above, if staff car is admissible, such employees may exercise option to avail staff car or higher rate of Transport Allowance @ Rs.15750/- as admissible to the Officers drawing pay in Level-14 & above of the Pay Matrix in terms of this Department's O.M. dated 07.07.2017. Transport Allowance in lieu of staff car shall be at the rate of Rs.15750/- per month plus Dearness Allowance only and not at the double of this rate.

5.4. The Transport Allowance at double the normal rates shall be admissible irrespective of whether the eligible Government employees are residing within campus (housing the place of work and residence) or residing in a Government/ Private accommodation within one kilometer of the office.

5.5. Assessment of disability and Certified Medical Authority concerned who issue the Disability certificate, would be with reference to Notification No. 16-09/2014 –DD-III dated 04.01.2018 issued by D/o Empowerment of Persons with Disabilities (Divyangjan) and any subsequent amendments thereto. However, in case of any doubt with regard to assessment of disability and issue of Disability certificate, the case may be referred to the Head of Department concerned for particular disability in a Government Civil Hospital.

File No. Z-28015/7/2025-PMSSY-IV (Computer No. 8314093)
Generated from eOffice by SANKAR GARG, SO(SG)-PMSSY-IV-MOHFW, SECTION OFFICER, DOHFW DEPARTMENT on 18/07/2025 04:36 pm

6. **Admissibility of Transport Allowance at double the normal rate during different circumstances:**

6.1. During leave: The allowance will not be admissible for the calendar month(s) wholly covered by leave.

6.2. During deputation abroad: The allowance will not be admissible during the period of deputation abroad.

6.3. During training, tour, etc.: If an employee with Benchmark Disability, is absent from the Headquarters/Place of posting for full calendar month(s) due to training, tour, etc., he/she will not be entitled to any Transport Allowance during that/those calendar month/months. However, If the absence does not cover any calendar month(s) in full, Transport Allowance at double the normal rate, will be admissible for full month.

6.4. During training treated as duty: In case the training is treated as duty, the allowance may be granted during such training, if no Transport Facility/Travelling Allowance/Daily Allowance is provided for attending the training institute. During official tour in the training course, the allowance will not be admissible when the period of the tour covers the whole calendar month. Also, during training abroad, no Transport Allowance will be admissible when the period of such training covers the whole calendar month.

6.5 During inspection/survey duty within the city but exceeding 8 kms from the Headquarters OR during continuous field duty either in or outside the Headquarters: In case the employee gets Road Mileage/Daily Allowance or free transportation for field /inspection/survey duty or tour for a period covering the whole calendar month, he/she will not be entitled to Transport Allowance at double the normal rate during that calendar month.

6.6 During vacation: The person with Benchmark Disability covered under Vacation staff is entitled to Transport Allowance at double the normal rate provided no free transport facility is given to such staff. However, the allowance shall not be admissible when such vacation spell, including all kinds of leave, envelops the entire calendar month(s).

6.7 During suspension: As a Government employee under suspension is not required to attend office, he/she is not entitled to Transport Allowance during suspension where suspension covers full calendar month(s). This position will hold good even if the suspension period is finally treated as duty. Where suspension period covers a calendar month partially, Transport Allowance at double the normal rate payable for that month shall be reduced proportionately.

Appendix

List of Orders on Transport Allowance at double the normal rates- superseded by this OM

Sr. No.	O.M. No.	Date	Subject
1.	19029/1/78-E.IV	31/08/1978	Grant of Conveyance Allowance to Blind and Orthopaedically Handicapped Central Government Employees.
2	19029/1/78-E.IV(B)	03/12/1979	Grant of Conveyance Allowance to Blind and Orthopaedically Handicapped CGEs
3	19029/1/78-E.IV (B)	05/10/1983	Grant of Conveyance Allowance to Blind CGEs.
4	21(1)97-E.II(B)	26/05/2000	Grant of Transport Allowance to Physically Handicapped CGEs.
5	21(1)97-E.II(B)	03/05/2002	Grant of Transport Allowance to CGE with Spinal Deformity.
6	21-1/2011-E.II(B)	05/08/2013	Grant of Transport Allowance to Orthopaedically Handicapped CGEs.
7	21(2)/2011-E.II(B)	19/02/2014	Extension of benefits of Transport Allowance @ double the normal rate to Deaf and Dumb CGEs.
8	20(2)/2016-E.II(B)	17/01/2017	Grant of Transport Allowance at double the normal rate to the Deaf & Dumb CGEs and also to Hearing Impaired CGEs.

No.A-27012/03/2017-Estt.(AL)
Government of India
Ministry of Personnel, P.G. and Pensions
Department of Personnel & Training

....

New Delhi, 16th August, 2017.

Subject: Recommendations of the Seventh Central Pay Commission – implementation of decisions relating to Special Allowance for child care for women with disabilities.

.....

Consequent upon the decision taken by the Government on the recommendations made by the Seventh Central Pay Commission for providing extra benefits to women employees with disabilities especially when they have young children and children with disability, the President is pleased to issue the following instructions:-

(i) Women with disabilities shall be paid Rs.3000/-per month as Special Allowance for Child care. The allowance shall be payable from the time of the child's birth till the child is two years old.
(ii) It shall be payable for a maximum of two eldest surviving children.
(iii) Disability means a person having a minimum Disability of 40% as elaborated in Ministry of Welfare's Notification No. 16-18/97-NI.I dated 1.6.2001 and amended from time to time.
(iv) The above limit would be automatically raised by 25% every time the Dearness Allowance on the revised pay structure goes up by 50%.

2. These orders shall be effective from 1st July, 2017.

3. Insofar as persons serving in the Indian Audit and Accounts Department are concerned, these orders issue in consultation with the Comptroller and auditor General of India.

Hindi version will follow.

Misra

(Navneet Misra)
Under Secretary to the Govt. of India

To

1. Ministries/Departments of the Government of India.

2. NIC with a request to upload the OM on the website of DoPT.

File No. Z-28015/7/2025-PMSSY-IV (Computer No. 8314093)
Generated from eOffice by SANKAR GARG, SO(SG)-PMSSY-IV-MOHFW, SECTION OFFICER, DOHFW DEPARTMENT on 18/07/2025 04:35 pm

DDA AIIMS PATNA <dda@aiimspatna.org>

Requirement of License issued by CDSCO/State Licensing Authorities in Procurement of Medical Devices by procurement agencies -reg

Ravi Kumar <ravi.kumar89@gov.in> Tue, Nov 25, 2025 at 6:18 PM
To: director <director@aiimsbhopal.edu.in>, madhabananda <madhabananda@gmail.com>, director <director@aiimsbhubaneswar.edu.in>, director <director@aiimsjodhpur.edu.in>, director <director@aiimspatna.org>, director <director@aiimsraipur.edu.in>, director <director@aiimsrishikesh.edu.in>, director <director@aiimsmangalagiri.edu.in>, directoraiimsnagpur <directoraiimsnagpur@gmail.com>, drppjoshi <drppjoshi@aiimsnagpur.edu.in>, edaiimsrbl <edaiimsrbl@gmail.com>, executivedirector <executivedirector@aiimsgorakhpur.edu.in>, ed <ed@aiimskalyani.edu.in>, director <director@aiimsbathinda.in>, director <director@aiimsdeoghar.edu.in>, director <director@aiimsbibinagar.edu.in>, director <director@aiimsbilaspur.edu.in>, shakti810505 <shakti810505@gmail.com>, director <director@aiimsjammu.edu.in>, ed <ed@aiimsrajkot.edu.in>, edaiimsrajkot2020 <edaiimsrajkot2020@gmail.com>, drmhraosvims1957 <drmhraosvims1957@gmail.com>, director <director@aiimsguwahati.ac.in>, sachimohanty <sachimohanty@rediffmail.in>, sharmadn <sharmadn@aiims.edu>, dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, dda <dda@aiimsjodhpur.edu.in>, dda <dda@aiimspatna.org>, dda <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, dda <dda@aiimsbathinda.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, ddaaiimsrbl <ddaaiimsrbl@gmail.com>, kpradip10 <kpradip10@gmail.com>, dda <dda@aiimskalyani.edu.in>, dda <dda@aiimsgorakhpur.edu.in>, dda <dda@aiimsdeoghar.edu.in>, officeaiimsdeoghar <office.aiimsdeoghar@gmail.com>, ddaaiimsbibinagar <dda.aiimsbibinagar@gmail.com>, dda <dda@aiimsbibinagar.edu.in>, dda <dda@aiimsbilaspur.edu.in>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, aps101982 <aps101982@rediffmail.com>, ddaaiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, dda <dda@aiimsguwahati.ac.in>, raj08642 <raj08642@gmail.com>, macprasad <mac.prasad@gmail.com>, ddaaiimsawantipora1 <ddaaiimsawantipora1@gmail.com>, dps <dps@hllhites.com>, shaileshbindal <shaileshbindal@hllhites.com>, abhijeetk <abhijeetk@hllhites.com>, ashwinikumar <ashwinikumar@hllhites.com>
Cc: kumarakhilesh <kumar.akhilesh@gov.in>, vijaykrgupta <vijaykr.gupta@nic.in>, VIKASH KUMAR GUPTA <vikas.kumar76@gov.in>, GUNJAN SHARMA <gunjan.s@nic.in>, pmssy01section <pmssy01section@gmail.com>

Sir,

Please find attachment on the above mentioned subject for your necessary compliance.

With regards,

Ravi Kumar,
Section Officer, PMSSY-I
M/o Health & Family Welfare
Nirman Bhawan, New Delhi

DGCI circular on medical device procurement.pdf
797K

Z-28016/113/2025-PMSSY-1

भारत सरकार

स्वास्थ्य एवं परिवार कल्याण मंत्रालय

स्वास्थ्य एवं परिवार कल्याण विभाग

पीएमएसएसवाई-I

निर्माण भवन, नई दिल्ली

दिनांक: 25.11.2025

To

i. Director/ Executive Director
All AIIMS under PMSSY;

ii. The CEO, M/s HITES

Subject: Requirement of License issued by CDSCO/State Licensing Authorities in Procurement of Medical Devices by procurement agencies -reg.

I am directed to forward herewith a copy of circular dated 17.11.2025 issued vide F. No. MED-13/87/2025 (copy enclosed) by Drug Controller General of India, CDSCO, DGHS on the subject mentioned above for necessary compliance and appropriate action.

Encl: As above.

भवदीय

25.11.25

(अखिलेश कुमार)
संयुक्त निदेशक(PMSSY)

File no. MED-13/87/2025-eoffice
Government of India
Directorate General of Health Services
Central Drugs Standard Control Organization
(Medical Device Division)

FDA Bhawan, Kotla Road,
New Delhi - 110002,
Dated 17 NOV 2025

Circular

Subject: Requirement of License issued by CDSCO/State Licensing Authorities in procurement of Medical Devices by procurement agencies-regarding

It has been brought to the notice of this office that the various procurement agencies including Hospitals are insisting for requirement of USFDA/CE certification as one of the requirements of technical bid for procurement of Medical Devices in the country.

Kind attention is invited that, the Ministry of Health and Family Welfare has come up with Medical Devices Rule,2017 under the Drugs and Cosmetics Act,1940 for regulation of Medical Devices in the country to ensure its quality, safety and performance. Currently, all the Medical Devices are regulated under said Rule and license is a mandatory requirement for its import, manufacturing, sale and distribution in the country. No Medical Devices can be sold in India without valid license obtained from Licensing Authorities. Based on the risk, Medical devices are classified into four categories viz. low risk Class A, low to moderate risk Class B, Moderate to high risk Class C and high risk Class D.

The manufacturing license for risk Class A & risk Class B medical devices and sale license for all risk class of Medical devices are issued by the concerned State/UT Licensing Authorities (SLAs). The Import license for all risk class of Medical devices and manufacturing license for risk Class C & risk Class D are issued by the Central Licensing Authority i.e. Central Drugs Standard Control Organization(CDSCO) based on the detailed technical review & conformance of Quality Management System in manufacturing of Medical Devices. The applicant shall obtain relevant license from the Concerned Licensing Authorities for sale and distribution of Medical Devices in the country.

In light of the above, all the procurement agencies including Hospitals, Health Institutions, etc., are requested that the CDSCO license or the license issued by the State/UTs Licensing Authority under the Medical Devices Rules, 2017, shall be made mandatory as a part of the requirements for procurement of Medical Devices, without which the medical device cannot be sold in the country. Any other certifications which is required by the procurement agency should be over and above of CDSCO or SLA Licensing Authority approval, under the said rules.

(Dr. Rajeev Singh Raghuvanshi)
Drugs Controller General of India

To,

All Heads of the Institute/Organizations/Hospitals etc.

Copy for information to:

1. PPS to Secretary Health
2. PS to DGHS
3. PS to JS (R)

File No. [illegible] Generated from eOffice by [illegible]

DDA AIIMS PATNA <dda@aiimspatna.org>

Applicability of DoPT's instruction related to Technical Resignation in new AIIMS

pmssysection iv <pmssysectioniv@gmail.com> Tue, Nov 25, 2025 at 4:23 PM
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, madhabananda@gmail.com, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, drppjoshi@aiimsnagpur.edu.in, Executive Director Raebareli <edaiimsrbl@gmail.com>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, "Prof. Dr. D.K. Singh, Director" <director@aiimsbathinda.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, "Dr.Shakti kumar Gupta" <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, ed@aiimsrajkot.edu.in, edaiimsrajkot2020@gmail.com, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, sachimohanty@rediffmail.in, "Sharma, DN" <sharmadn@aiims.edu>
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, "Dy Director Administration AIIMS, Raebareli" <ddaaiimsrbl@gmail.com>, "Dr. Pradip Kumar" <kpradip10@gmail.com>, dda@aiimskalyani.edu.in, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, dda@aiimsbilaspur.edu.in, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, aps101982@rediffmail.com, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, dda@aiimsguwahati.ac.in, raj08642@gmail.com, Mukesh Kumar <mac.prasad@gmail.com>, ddaaiimsawantipora1@gmail.com, ":" <Ak.biswas57@nic.in>, Arvind Thakur <arvind.thakur@nic.in>, Devender DKumarGothal <dev.gothal@gov.in>, a.adil60@gov.in, premprakash.bth@gov.in, Vaishali Vinayak <vaishali.vinayak@gov.in>, Amit Batra <amit.batra@gov.in>, manoj@ndma.gov.in, r.ahul@gov.in

Sir/ Madam,

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officers of PMSSY-IV Section at - arvind.thakur@nic.in;ak.biswas57@nic.in; premprakash.bth@gov.in; dev.gothal@gov.in; a.adil60@gov.in; vaishali.vinayak@gov.in; amit.batra@gov.in; manoj@ndma.gov.in; r.ahul@gov.in; sup15.81997@gov.in;

Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

Technical Resignation_251125_152726.pdf
528K

Z-28016/192/2020-PMSSY-IV-Part(1)(8149336)
Government of India
Ministry of Health and Family Welfare
Department of Health and Family Welfare
(PMSSY Division)
***

Nirman Bhawan, New Delhi
25.11.2025

To,

Executive Directors of all new AIIMS.

Sub: Applicability of DoPT's instructions related to Technical Resignation in new AIIMS

Sir/Madam,

I am directed to convey that the competent authority in the Ministry has approved adoption of DoPT's Rules/Instructions on Technical Resignation as part of the service conditions of Faculty/Non-Faculty of all new AIIMS. Accordingly, the consequent benefits of lien, pay protection, applicability of pension scheme, GPF transfer etc. shall be in accordance with the instructions on Technical Resignation stipulated in DoPT's OM No.DOPT-1669266628362 dated 24.11.2022 and instructions on the subject matters issued from time to time.

2. It is clarified that the pay protection granted to Faculty/staff under Technical Resignation shall not be considered to decide his/her seniority in the new organization as the seniority is decided in term of Regulation 26 of AIIMS Regulations 2019, which provides that *"the seniority of employees of the Institute in each category shall be determined by the order of merit in which they were selected for appointment to the post in question, those selected on an earlier occasion being ranked senior to those selected later"*.

Yours faithfully,

(Arvind Thakur)
Deputy Secretary to the Government of India

DDA AIIMS PATNA <dda@aiimspatna.org>

Fwd: Powers for granting administrative approval and financial sanction for incurring expenditure from the Grants-in-aid.

Director . <director@aiimspatna.org> Wed, Nov 26, 2025 at 11:37 AM
To: DDA AIIMS PATNA <dda@aiimspatna.org>, Finance & Chief Accounts Officer <fcao@aiimspatna.org>

Sd/-
Prof. (Brig.) Dr. Raju Agarwal
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109

---------- Forwarded message ---------
From: **pmssysection iv** <pmssysectioniv@gmail.com>
Date: Tue, Nov 25, 2025 at 2:37 PM
Subject: Powers for granting administrative approval and financial sanction for incurring expenditure from the Grants-in-aid.
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, <madhabananda@gmail.com>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, <drppjoshi@aiimsnagpur.edu.in>, Executive Director Raebareli <edaiimsrbl@gmail.com>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Prof. Dr. D.K. Singh, Director <director@aiimsbathinda.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, Dr.Shakti kumar Gupta <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, <ed@aiimsrajkot.edu.in>, <edaiimsrajkot2020@gmail.com>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, <sachimohanty@rediffmail.in>, Sharma, DN <sharmadn@aiims.edu>
Cc: Arvind Thakur <arvind.thakur@nic.in>, <premprakash.bth@gov.in>, <manoj@ndma.gov.in>, <r.ahul@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officers of PMSSY-IV Section at - premprakash.bth@gov.in; manoj @ndma.gov.in; r.ahul@gov.in;
Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

ED AIIMS.pdf
239K

Z-28016/65/2024-PMSSY-V (8271024)
Government of India
Ministry of Health and Family Welfare
Department of Health and Family Welfare
(PMSSY Division)
***

Nirman Bhawan, New Delhi
25.11.2025

To,

Executive Directors of all new AIIMS.

Sub: Powers for granting administrative approval and financial sanction for incurring expenditure from the Grants-in-aid

In supersession of this Ministry's letter No. Z-28016/146/2023-PMSSY-IV dated 15.06.2017, the competent authority has approved the following arrangement for incurring expenditure from the Grants-in-aid being allocated to new AIIMS by the Central Government:

(i) Executive Directors of new AIIMS set up under the AIIMS Act, 1956 (as amended) are authorized for granting administrative approval and financial sanction for incurring expenditure upto Rs. 5.0 crore from the Grants-in-aid for procurement of works, goods, consultancy services and non-consultancy services.

(ii) All cases of expenditure on procurement of works, goods, consultancy services and non-consultancy services exceeding Rs. 5.0 crore shall be placed by the respective Institutes before the Standing Finance Committee for consideration and approval.

2. The Executive Directors may consider delegating the aforesaid administrative and financial powers to authority(ies) subordinate to Executive Director with prior approval of the Governing Body.

3. The above powers for incurring expenditure shall be subject to compliance of provisions contained in General Financial Rules, Manuals of Procurement on Works, Goods, Consultancy services and Non-Consultancy Services issued by the Department of Expenditure and other GoI instructions on the matter issued from time to time.

Yours faithfully,

(Arvind Thakur)
Deputy Secretary to the Government of India

DDA AIIMS PATNA <dda@aiimspatna.org>

Fwd: Compliance in respect to the Information Security Policy for Healthcare (Version 1.0) and security guidelines for consultants and outsourced staff -reg.

3 messages

Director . <director@aiimspatna.org> Fri, Dec 5, 2025 at 11:27 AM
To: DDA AIIMS PATNA <dda@aiimspatna.org>

Sd/-
Prof. (Brig.) Dr. Raju Agarwal
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109

---------- Forwarded message ---------
From: **eHealth Section** <telmed-mohfw@gov.in>
Date: Thu, Dec 4, 2025 at 4:00 PM
Subject: Compliance in respect to the Information Security Policy for Healthcare (Version 1.0) and security guidelines for consultants and outsourced staff -reg.
To: director <director@aiimsbhopal.edu.in>, director <director@aiimsbhubaneswar.edu.in>, director <director@aiimsjodhpur.edu.in>, director <director@aiimspatna.org>, director <director@aiimsraipur.edu.in>, director <director@aiimsrishikesh.edu.in>, director <director@aiimsmangalagiri.edu.in>, directoraiimsnagpur <directoraiimsnagpur@gmail.com>, drppjoshi <drppjoshi@aiimsnagpur.edu.in>, Edaiimsrbl <edaiimsrbl@gmail.com>, executivedirector <executivedirector@aiimsgorakhpur.edu.in>, Ed <ed@aiimskalyani.edu.in>, Director <director@aiimsdeoghar.edu.in>, Director Bibinagar <director@aiimsbibinagar.edu.in>, Director <director@aiimsbilaspur.edu.in>, sharmadn <sharmadn@aiims.edu>, shakti810505 <shakti810505@gmail.com>, director <director@aiimsjammu.edu.in>, Drmhraosvims1957 <drmhraosvims1957@gmail.com>, director <director@aiimsguwahati.ac.in>, madhabananda <madhabananda@gmail.com>, sachimohanty <sachimohanty@rediffmail.in>, sharmadn <sharmadn@aiims.edu.in>, med rmlh <med.sup.rmlh@gmail.com>, preetichauhan74 <preeti.chauhan74@nic.in>, Sameek Bhattacharya <sameek.bhattacharya@rmlh.nic.in>, vivekgupta <vivekgupta@aiims.gov.in>, director <director@vmmc-sjh.nic.in>, MEDICAL SUPERINTENDENT <msoffice@vmmc-sjh.nic.in>, N N Director <director-lhmc@gov.in>, Anjana Rajkumar <director-cghs@cghs.nic.in>, Srinivas.M <director@aiims.gov.in>, rrcrishikesh <rrcrishikesh@aiimsrishikesh.edu.in>, rrckemh <rrckemh@kem.edu>, rrcpgimer <rrcpgimer@gmail.com>, rrc bhu <rrc.ims.bhu@gmail.com>, rrceastims <rrceastims@bhu.ac.in>, Director Neigrihms <director-neigrihms@gov.in>, Director JIPMER <director@jipmer.edu.in>, Rakesh Lucknow <director@sgpgi.ac.in>, director <director@rcctvm.gov.in>, dda <dda@pgimer.edu.in>, drabhyuday <drabhyuday@aiimspatna.edu.in>, pps <pps@aiimsrishikesh.edu.in>, srprogrammer <srprogrammer@aiimsbhopal.edu.in>, dryatirajfmt <dr.yatiraj.fmt@aiimsbilaspur.edu.in>, ciso <ciso@aiimskalyani.edu.in>, Head IT <head.it@aiimsjammu.edu.in>, drmohanraj <drmohanraj@aiimsgorakhpur.edu.in>, admin <admin@aiimsnagpur.edu.in>, ciso <ciso@aiimsrbl.edu.in>, debboruah <debboruah@aiimsguwahati.ac.in>, rohitbio <rohit.bio@aiimsbibinagar.edu.in>, ciso <ciso@aiimsraipur.edu.in>, IT Cell <itdept@aiimsbhubaneswar.edu.in>, mundraa <mundraa@aiimsjodhpur.edu.in>, dhootr <dhootr@aiimsjodhpur.edu.in>, registraraiimsmadurai <registrar.aiimsmadurai@gmail.com>, drrajepath <drraje.path@aiimsmadurai.edu.in>, IT Bathinda <itcell.support@aiimsbathinda.edu.in>, Dinesh Kumar <dinesh.kumar14@nic.in>
Cc: Madhukar Kumar Bhagat <jsehealth-mohfw@gov.in>, ANKITA MISHRA BUNDELA <js-pmssy-mohfw@gov.in>, Manashvi Kumar <jstraining-mohfw@gov.in>, REENA SHARMA <reena.sharma80@gov.in>, Pawan Kumar <pawan.kumar13@nic.in>, Piyush Malyan <piyush.malyan@gov.in>

Sir/Madam,

Kindly refer to the attached **OM dated 04th December, 2025** regarding the subject cited above. In this regard you are requested that suitable instructions be given to all concerned officers/stakeholders of your Organization for the successful implementation of these guidelines/policy.

2. A meeting chaired by the Joint Secretary (eHealth) has already been held at RML, VMMC & SJH, LHMC, CGHS, and AIIMS Delhi on the implementation of these guidelines. Accordingly, an action-taken report on the same may be submitted by 10-12-2025.

Regards
Swapnil Prabhat
eHealth Section
Ministry of Health & Family welfare
Room No.-213, D-wing, Nirman Bhawan
New Delhi-110011
Tel No.-23062263

4 attachments

OM dt 04.12.2025 regarding ISMS policy-.pdf
540K

Information Security Policy for Healthcare_v1.0 as on 07072025-2.pdf
3705K

Information Security Guidelines for Consultants_v1.0 as on 07072025 (1)-2.pdf
1056K

OM dated 07th July 2025(All AS,JS).pdf
561K

DDA AIIMS PATNA <dda@aiimspatna.org> Fri, Dec 5, 2025 at 5:51 PM
To: Rishi Bhushan <rishi.bhushan@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507
[Quoted text hidden]

4 attachments

OM dt 04.12.2025 regarding ISMS policy-.pdf
540K

Information Security Policy for Healthcare_v1.0 as on 07072025-2.pdf
3705K

Information Security Guidelines for Consultants_v1.0 as on 07072025 (1)-2.pdf
1056K

OM dated 07th July 2025(All AS,JS).pdf
561K

DDA AIIMS PATNA <dda@aiimspatna.org> Tue, Dec 9, 2025 at 6:51 PM
To: telmed-mohfw@gov.in
Cc: "Director ." <director@aiimspatna.org>, Madhukar Kumar Bhagat <jsehealth-mohfw@gov.in>, ANKITA MISHRA BUNDELA <js-pmssy-mohfw@gov.in>, Manashvi Kumar <jstraining-mohfw@gov.in>, REENA SHARMA

<reena.sharma80@gov.in>, Pawan Kumar <pawan.kumar13@nic.in>, Piyush Malyan <piyush.malyan@gov.in>, Principal Private Secretory <pps@aiimspatna.org>
Bcc: dda ps <dda.ps@aiimspatna.org>

Sir/Madam,

Please find the attachment for your perusal and necessary action.

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

[Quoted text hidden]

COMPLIANCE IN RESPECT OF INFORMATION SECURITY POLICY FOR HEALTHCARE.pdf
1982K

F.No.:T-21016/60/2023-eHealth
Government of India
Ministry of Health and Family Welfare
eHealth section

Nirman Bhawan, New Delhi
Dated the 4th December, 2025

OFFICE MEMORANDUM

Subject:- Compliance in respect to the Information Security Policy for Healthcare (Version 1.0) and security guidelines for consultants and outsourced staff -reg.

The undersigned is directed to refer to D.O No. M-11011/6/2015-eHealth, dated 7th July, 2025 from Joint Secretary (eHealth), MoHFW, regarding the subject mentioned above and to state that e-Health Division of the Ministry of Health and Family Welfare, in consultation with NRCeS, CDAC Pune, had prepared an Information Security Policy for Healthcare and security guidelines for consultants and outsourced staff. A copy of these guidelines is attached at Annexure for your reference and compliance.

2. In this regard, it is stated that these guidelines are to be mandatorily implemented in your respective Organizations. It is therefore requested that suitable instructions to be given to all concerned officers/stakeholders of your Organization for the successful implementation of these guidelines/policy.

3. Further, a meeting chaired by the Joint Secretary (eHealth) has already been held at RML, VMMC & SJH, LHMC, CGHS, and AIIMS Delhi on the implementation of these guidelines. Accordingly, an action-taken report on the same may be submitted by 10-12-2025.

4. This issues with the approval of the Competent authority.

Yours faithfully,

(Pawan Kumar)
Under Secretary to the Government of India
Tel: 011-23062666

Encl: As above

To,

1. Director, AIIMS, Delhi
2. Director, Dr. RML Hospital, Delhi
3. Director, VMMC & SJH, Delhi
4. Director, LHMC, Delhi
5. Director, CGHS, MoHFW
6. Executive Directors of all AIIMS

7. Director, RRC SGPGIMS
8. Director, RRC (EAST) IMS, BHU
9. Director, RRC PGIMER
10. Director, RRC NEIGRIHMS
11. Director, RRC KEM, Mumbai
12. Director, RRC JIPMER, Puducherry
13. Director, RRC Trivandrum Medical College, Thiruvananthapuram

Copy to:

1. Sr. PPS to JS (eHealth)
2. Dy. CISO, NIC, MoHFW



Security Guidelines for Appointment and Discharge of Official Functions by Consultants/ Outsourced Staff in Ministry of Health and Family Welfare (MoHFW)

Reference: OM No. Z.28015/21/2023.Estt-II dated 08.11.2024 issued by Establishment-II Section)

Version 1.0

July 2025

भारत सरकार/Government of India
स्वास्थ्य एवं परिवार कल्याण/Ministry of Health and Family Welfare
Nirman Bhawan
New Delhi-110001
E-mail: telmed-mohfw@gov.in

For limited circulation (Information Security Guideline No. 1/2025)
@eHealth Division, MoHFW

Table of Contents

Sections	Page No
Section 1: Objectives	1
Section 2: Engagement of Authorized Service Provider and Outsourced Staff	1
Section 3: Onboarding of Consultants and Outsourced staff	3
Section 4: Compliances	5
Section 5: Non-compliance and Violation of Policy	8
Section 5: Exit Management	9
Annexures o Annexure I: Joining Formalities o Annexure II: Exit Formalities o Annexure III: Non-Disclosure Agreement o Annexure IV: NICSI Hiring Guidelines	11

Section 1: Objectives

1.1 This guideline is established to ensure the security of information and associated assets while appointment and performance of official functions by consultants and outsourced staff. Its primary objective is to uphold the confidentiality of information, which the appointed consultants, outsourced staff or the agencies from which they are hired may come across during the performance of the official functions.

1.2 The guideline mandates the implementation of robust security controls across data, applications, digital and non-digital devices infrastructure, and endpoint as well as system integrity to prevent unauthorized access and ensure comprehensive data protection.

Section 2: Engagement of Authorized Service Provider for Hiring of Consultants/ Outsourced Staff

2.1 This guideline highlights a general protocol to assist the Divisions of MoHFW in maintaining appropriate security posture in hiring of consultants and outsourced staff as well as during the performance of official functions by them.

2.2 For the hiring of consultants and outsourced staff at MoHFW, the Divisions of MoHFW should follow the appropriate hiring/procurement guidelines issued by the Government of India (GoI) from time to time including GFR guidelines[1], etc. Necessary prior approvals from the competent authority and associated financial approvals should be obtained with the approval of Integrated Finance Division (IFD) and MoHFW.

2.3 To recruit technical consultants, as a best practice, the divisions may constitute an interview panel with representatives from the Division concerned and/or hiring agency etc so as National Informatics Centre (NIC) or any other authorized associated institutions/

[1] Government of India, Ministry of Finance Department of Expenditure, Manual for Procurement of Goods 2017; Section 3.2.2 Code of Integrity for Public Procurement & Section 3.2.3 Obligations for Proactive Disclosures
Manual for Procurement of Goods 2024; Section 3.2 Code of Integrity for Public Procurement

division and or hiring agency etc. so as to conduct the individual interviews of the prospective resource persons.

2.4 Appropriate and prior due diligence for background check and police verification of all consultants and outsourced staff must be done. However, time frame for such checks and police verification may be extended by the Divisional heads in case of exigencies. The onus of conducting comprehensive background checks and police verifications of all proposed candidates to be interviewed/hired should be on the service provider/hiring agency or outsourced agency.

2.5 Further, the service provider/hiring agency must ensure that consultants and outsourced personnel undergo appropriate information and security training before joining the division.

2.6 At the time of joining their respective officers all consultants and outsourced personnel must provide a formal undertaking to uphold the confidentiality and integrity of the organization's data. A recommended format of non-disclosure and confidentiality undertaking is given as per Annexure-I.

2.7 Preference may be given to candidates who have completed a recognized public course in the specific domain in accordance with her/his terms of reference and Information Security course or possess prior experience in Information Security having worked within a Government Department.

2.8 For reference related to guidance on the hiring of personnel from National Informatics Centre Services Inc (NICSI), refer to the NICSI hiring guidelines attached in Annexure IV.

Section 3: Onboarding of Consultant/ Outsourced Staff

3.1 Hiring of consultants or outsourced employees for the Ministry of Health and Family Welfare (MoHFW) shall be conducted through approved or empaneled agencies or by the respective Project Directors (PDs) of the Ministry, following the prescribed procedures.

3.2 All candidates must undergo thorough background checks.

3.3 **Consultants,** particularly technical experts **engaged in sensitive, policy-level assignments must submit their credentials in advance to the Ministry of Home Affairs (MHA)** in a formalized format and as per the specified address. In cases involving the recruitment of retired Government officials, vigilance clearance from the respective Ministry or Department must be obtained before their appointment.[2]

3.4 **All consultants must sign a Non-Disclosure Agreement (Annexure-III)** before the commencement of their roles. This agreement includes a mandatory two-year cooling-off period after the conclusion of their Government contract, prohibiting them from joining foreign missions, firms, or think tanks during this period. [2]

3.5 A comprehensive security briefing must be provided to all consultants upon hiring. This briefing will cover critical security measures, including dos and dont's, and specific precautions for remote work.

3.6 Following consultants' recruitment, a formal request for an authorized entry pass to the MoHFW must be submitted to the Ministry of Home Affairs (MHA) for approval. Consultants and outsourced employees are required to use this pass and adhere to the biometric recognition system for entry into the Ministry premises. Consultants are required to comply with the working hours prescribed by Government of India and should seek prior approval for staying in office beyond working hours.

[2] OM No. Z.28015/21/2023.Estt-II dated November 8, 2024 of MoHFW

3.7 All consultants and outsourced employees are mandated to undergo training on the Information and Cyber Security guidelines of the MoHFW.

3.8 Wherever permitted, consultants and outsourced employees may participate in virtual meetings related to MoHFW work, utilizing approved platforms such as Microsoft Teams or Zoom.

3.9 The user IDs including the email IDs provided by the MoHFW are strictly for official use and must not be employed for any personal purposes.

3.10 Access to Ministry meetings, documents, computers, and information shall be granted to consultants on a strict need-to-know basis, following specified access control norms.

3.11 A comprehensive list of consultants and outsourced employees engaged in the division must be maintained, including their demographic details, contact information educational qualifications, assigned work profiles, the nature of data handled (e.g., public, ministerial limited access, confidential, secret, top secret) along with copies of their CVs, and recent photographs. Additionally, work allocations for all consultants must be systematically documented and shared across the relevant divisions.

Section 4: Compliances

(a) Physical and access control of hardware

4.1 Consultants and outsourced employees must use an authorized pass to enter the Ministry of Health and Family Welfare (MoHFW). If they are required to stay in the MoHFW premises beyond standard working hours or on holidays, prior approval must be obtained from competent authority.

4.2 Access to data or applications should be only through the allotted device using MoHFW login credentials, and if necessary, through a Virtual Private Network (VPN) after obtaining due approval from the competent authority.

4.3 Only the authorized Wi-Fi connection provided by MoHFW should be used. Personal external Wi-Fi devices or network equipment, such as dongles, are not permitted for accessing the internet or connecting to hardware within MoHFW premises. Personal mobile phones or iPads must not be used to access MoHFW systems. All laptops, desktops, and other electronic devices officially provided must undergo hardening to ensure security compliance.

(b) Access Rights

4.4 Access to the Ministry of Health and Family Welfare (MoHFW) portals must be conducted exclusively through authorized devices and credentials allocated by the MoHFW. Data access should be strictly based on the individual's role and the established policies. Furthermore, data should only be accepted if it is shared through proper channels approved by the MoHFW.

(c) Data Handling

4.5 Data must be utilized solely for the purposes specified by the Ministry of Health and Family Welfare (MoHFW). Any use of data beyond these specified purposes is strictly

prohibited to ensure compliance with MoHFW guidelines and to maintain data integrity and security.

(d) Data Transfer

4.6 Data transfer must strictly adhere to the guidelines established by the Ministry of Health and Family Welfare (MoHFW). Any transfer of data should be conducted in accordance with protocols to ensure security and compliance. Additionally, if there is a need to carry hardcopies of any documents outside the MoHFW premises, prior approval must be obtained from the relevant authorities.

4.7 The use of the official printer provided by the MoHFW is restricted to printing documents that are directly related to MoHFW activities.

4.8 Consultants and outsourced employees should not use any social media platforms. to circulate data generated within the MoHFW.

4.9 The use of unauthorized electronic gadgets, including but not limited to hard disks, pen drives, and bluetooth devices, for transfer of data or information pertaining to the MoHFW is also strictly prohibited.

4.10 Consultants and outsourced employees are not permitted to publish any data generated by the MoHFW in the form of external reports or documents without explicit authorization.

(e) Data Storage

4.11 All data pertaining to the Ministry of Health and Family Welfare (MoHFW) must be stored exclusively on authorized cloud storage platforms or data storage devices provided officially. To ensure data security and compliance with MoHFW guidelines, storing MoHFW data on unapproved cloud storage or non-official devices is strictly prohibited.

(f) Social platform

4.12 The official email ID and credentials provided by MoHFW should not be used to access any social media platforms. They may be strictly prohibited from taking and posting any pictures or videos taken within premises of MoHFW, delegates visits and other official functions of MoHFW in their individual accounts or at social media accounts etc,

4.13 Employees and consultants must refrain from expressing any personal views on social media platforms pertaining to MoHFW. Furthermore, circulating any data or information related to MoHFW on social media platforms is strictly forbidden.

Section 5: Non-compliance and Violation of policy

5.1 Any non-compliance or violation of policy listed, but not limited to those highlighted above, may be dealt with strict actions in terms of the provisions of the employment-contract including termination of the engagement. Further, wherever applicable the provisions of the Digital Personal Data Protection (DPDP) Act 2023, the Information Technology (IT) Act 2000, the Information Technology (Amendment) Act 2008 and the Bharatiya Nyaya Sanhita 2023 shall apply and provisions and penalties as thereby specified may be invoked. Some examples of specific instances of non-compliance violation are as follows:

1. **Unauthorized Access:** Accessing restricted areas, information, or data without proper authorization. This also includes physical access to secure areas and digital access to unauthorized information.
2. **Data mishandling:** This include mishandling of sensitive data or failure to follow data protection protocols. This could include unauthorized sharing of personal data, failure to encrypt sensitive information, or not reporting data breaches timely.
3. **Non-Adherence to Protocols:** This could include failure to adhere to established security protocols during work hours within the MoHFW. This includes not following procedures for data access, transfer, and storage, or using unauthorized devices to access MoHFW systems.

Section 6: Exit Management

6.1 The outgoing consultant or outsourced personnel must follow a defined process to complete the exit management protocol.

6.2 A prior notice period of either one month or fifteen days, as specified in the contract, must be provided by the consultant or outsourced personnel.

6.3 The outgoing consultant should conduct a 'knowledge transfer' (KT) of information, documents and procedural known how to an existing team member within the division for a minimum duration of fifteen days. The Knowledge Transfer should include transfer of data files, records, explanation of work handled etc. Further the consultant must prepare a detailed report of all work and deliverables completed during his/her tenure. This should be stored in the MoHFW database and duly intimated to the relieving officials and supervisory officials.

6.4 Upon completion of the Knowledge Transfer, all logical access, including User ID and password, access to portals, APIs, databases, and network equipment, should be revoked. All IT assets allocated to the outgoing consultant should be transferred to an existing team member or division. Further the outgoing consultants is required to return all allocated documents, hardware, and IT equipment, such as desktops or laptops. At the time of relieving, the consultant's User ID and access rights shall be deactivated.

6.5 Physical access to the Ministry of Health and Family Welfare (MoHFW) premises should be blocked on the consultant's last working day unless prior approval for extended access has been obtained. The physical access card must be surrendered, and the biometric attendance system to be disabled.

6.6 All stakeholders must be informed about the consultant's departure by the respective division. Additionally, the consultant must submit a declaration confirming the non-retention of any unauthorized data.

6.7 A declaration must also be submitted by the consultant regarding the return of hardware, requests for access removal, and an assurance that confidential data will not be used for any unauthorized purposes.

6.8 A joint exit interview should be conducted, during which the consultant should provide a declaration confirming the handover of all documents, hardware, passwords, and other relevant items. This declaration should be countersigned by the consultant's reporting officer. The entire exit process should be verified using a checklist maintained by the concerned Program Division detailed in Annexure II.

Annexure – I

Joining Checklist

I _____ (Name, Designation & Division of the Employee) declare that I will:

Physical Access

- use an authorized pass for entry to MoHFW,
- use the biometric and facial recognition system to access the premises,
- take prior approval if asked to stay in the premises after working hours,
- take prior approval if asked to report on a leave day,
- adhere to work timings prescribed by the Government of India (GoI),
- only attend virtual meetings using approved platforms for related work due to the sensitive nature of data,
- not allow any unauthorized personnel to enter the premises,

Hardware Access

- access data only on the allotted device using login credentials and Virtual Private Network (VPN),
- use only authorized Wi-Fi connection provided by MoHFW,
- do not carry any personal external Wi-Fi devices/network equipment such as dongles for accessing the internet,
- do not use my personal mobile phone/I-pad to access,

Data Management Guidelines

1. **Data Access**

- access the portal through authorized devices and credentials only,
- render duties as per the role provided,
- access the data based on role and policies,
- accept data only shared through proper channels i.e., approved by the CHI and eHealth division

2. **Data Handling**

- use data only for the purpose defined by the MoHFW,
- don't access Illegal/blocked Websites, portals, applications, open databases in MoHFW network

3. **Data Transfer**

- transfer data as per the MoHFW guidelines only,
- take Prior approval if hardcopies need to be carried outside the MoHFW premises,
- use the official printer provided to print only MoHFW documents,
- not use any social media platform to circulate data generated in MoHFW,
- not use any unauthorized electronic gadgets (hard disks, pen drives, Bluetooth devices) for the transfer of data or information,
- not publish the data in any external report/document,

4. **Data Storage**

- store data on an authorized cloud storage,
- not store data on any external cloud/external devices,

Social Media

- not click any picture or video,
- not use credentials for personal use on any social media platform,
- not post any confidential data on any social media platform,
- not express any personal views on social media platforms pertaining to the data,
- not circulate any data or information on any social media platform,

I have read and will adhere to all the above points and guidelines.

Name:

Signature:

Date:

Annexure – II

Exit Checklist

Name:	
Date of Relieving:	
Name of Reporting Manager:	
Designation & Division of Reporting Manager:	

This is to confirm that the employee has completed the following tasks/ handed over the below mentioned items.

(Kindly Note: This sheet should get signed in the sequence given below)

Reporting Manager			
	Y	N	Remarks
Has completed the tasks at hand			
Has transferred the knowledge to the nominated colleague			
Has transferred all the IT assets, documents, books, packages, confidential material etc., to the nominated colleague			
Has prepared a repository of all work/ deliverables			

Information Technology			
	Y	N	Remarks
Blocked email ID access			
Blocked to MoHFW network (Wifi, LAN, etc.)			
Blocked access to all APIs, databases			

Blocked access to other program division portal			

Administration			
	Y	N	Remarks
Has submitted MoHFW Access Card to eHealth Division			
Has submitted RFID Cards, Access Card etc.to the concerned division			
Confirmation of deletion of Facial recognition and biometric access from the MoHFW database.			

Signature by Reporting Manager **Signature by Resource**

Date:

Annexure – III

Non-Disclosure Agreement

This agreement is effective this date <dd/mm/yyyy> by and between MoHFW with its registered office at Nirman Bhawan, New Delhi

AND

<Consultant/Outsourced> <Recipient> with its registered office at <Full address with Pin>

1. **Disclosing Party**: During the term of this Agreement, Recipient agrees to receive from <SHORT NAME 1> the following information ("Confidential Information") set forth in Section 2.

2. **Confidential Information**: Confidential Information is all information that is described in this Section or that: (i) is marked as confidential at the time of disclosure; or (ii) is unmarked but treated as confidential at the time of disclosure; or (iii) is accessed or obtained by the Recipient or disclosed to the Recipient, whether inadvertently or not, whether by direct or indirect, oral or written communication to the Recipient.

   Description of Confidential Information: The Confidential Information disclosed under this Agreement is described as:
   <SHORT NAME 1> or its customer's trade secrets; financial information, including pricing; technical information, including research, development, procedures, algorithms, data, designs, and know-how; and business information, including operations, planning, marketing interests, products and any other information shared or you have access in the course of mutual business.

3. **Restrictions**: Recipient shall maintain the Confidential Information in strict confidence and disclose the Confidential Information only to its employees, subcontractors and consultants that have a need to know such Confidential Information and solely for the purpose described in Section 4., provided, that Recipient shall first have entered into a confidentiality agreement with such employees, subcontractors and consultants requiring such individuals to comply with this Agreement. The Recipient shall not disclose the Confidential Information to any third parties nor allow third parties access to the

Confidential Information. The Recipient shall not use the Confidential Information for any internal business use, except as mentioned in this Agreement, to the detriment of <SHORT NAME 1>

4. **Purpose**: Recipient shall make use of the Confidential Information only for the following purpose:

   Developing or presenting a proposal to MoHFW

   Modification of a party's product(s) to enhance compatibility with the other party's product(s).

5. **Confidentiality Period**: Recipient's duty to protect Confidential Information shall survive the termination/expiry of this Agreement. This Agreement shall be for a period of 5 years or the date of termination of contract, from the date of last disclosure.

6. **Disclosure Period:** This Agreement applies to the Confidential Information described in Section 2. that is disclosed between the Effective Date of this Agreement and five (5) years thereafter.

7. **Standard of Care**: Recipient shall afford such Confidential Information the same security and care in handling and storage as Recipient provides for its own confidential and proprietary information and data, but in any case, no less than reasonable care. Recipient agrees not to duplicate or otherwise copy and to return immediately at the <SHORT NAME 1>'s request all Confidential Information including any plans, design, documents or other tangible items (including electronic media) copied or derived from and containing Confidential Information.

8. **Exclusions**: Recipient shall not be liable for use or disclosure of any such Confidential Information if the same: (a) is in the public domain at the time it is disclosed or becomes a matter of public knowledge through no fault of Recipient; or (b) is known, as demonstrated by written documentation, to the party receiving it at the time of disclosure; or (c) is rightfully received by Recipient from a source other than the disclosing party

without a duty of confidentiality; or (d) is independently developed, separate from the activities undertaken pursuant to this Agreement, and such development can be verified through sufficient written documentation.

9. **Required Disclosures**: In the event Recipient is confronted with legal action to disclose Confidential Information received under this Agreement, the Recipient shall promptly notify the <SHORT NAME 1> in writing and shall reasonably assist the <SHORT NAME 1> in obtaining a protective order requiring that any portion of the Confidential information required to be Disclosed be used only for the purpose which a court issues an order, or for such other purpose as required by law.

10. **Warranty**: **NO WARRANTIES, INCLUDING WARRANTIES AGAINST INFRINGEMENT ARE MADE BY <SHORT NAME 1> UNDER THIS AGREEMENT. ANY INFORMATION EXCHANGED UNDER THIS AGREEMENT IS PROVIDED "AS IS".**

11. **No Other License:** Recipient does not acquire any intellectual property rights under this Agreement. No license is granted by <SHORT NAME 1> to Recipient under any patent, trademark, copyright or mask work other than as expressly set forth herein.

12. **Miscellaneous**

12.1 This Agreement contains the entire understanding of the parties and supersedes all other agreements or understandings with respect to the subject matter hereof. Any amendment to this Agreement must be in writing, signed by authorized representatives of each party, and expressly refer to this Agreement.

12.2 Upon five (5) days prior written notice, either party may notify the other that it no longer wishes to receive or provide Confidential Information. Any information received or provided by either party thereafter shall not be subject to the protection of this Agreement.

12.3 Upon the termination of this Agreement and at the written request and instruction of <SHORT NAME 1>, all Confidential Information furnished hereunder, including any

copies thereof, shall be either returned to <SHORT NAME 1> or destroyed and a certificate of destruction shall be timely provided by Recipient to <SHORT NAME 1>.

12.4 This Agreement does not create any agency or partnership relationship. Each party is responsible for its own expenses incurred as a result of any discussion between the parties.

12.5 This Agreement shall be governed by and construed in accordance with the laws of India and the parties submit to the exclusive jurisdiction of the courts in <Location Name>.

IN WITNESS WHEREOF, each party has caused this Agreement to be executed on its behalf by an officer or company employee thereunto duly authorized, all as of the date set forth above.

For <MoHFW>.	<Recipient Name>
By:_____	By:_____
Name:	Name:
Title:	Title:
Date:	Date:

Annexure – IV

Step by step process for getting the Work Order from NICSI

Step 1:

Client needs to fill the **Proforma Invoice** (PI) Request and send it to NICSI-PI DIVISION <pi@nicsi.nic.in> *(Format enclosed)*



Proforma Invoice (PI) Request Form.pdf

Step 2:

NICSI PI DIVISION will respond as per this PI Request Form (PIRF) received from the Client and share Proforma Invoice, Bank details for transferring the funds to NICSI and Template of Project Execution Form (PEF) to all Empaneled Vendors.



Project Execution Form (PEF).pdf



ICICI.pdf

Step 3:

Client needs to finalize the empaneled Vendor who will execute the work and transfer funds as per the amount mentioned in the Proforma Invoice. Client is also expected to send the Project Execution Form (PEF) duly filled with the fund transfer details and resource deployment details (project start & completion date) to the email id mentioned in PI document. *(Format enclosed)*

Step 4:

Once NICSI received funds and complete Project Execution Form (PEF) document they will add /create NICSI project code and will releasing the Work Order to respective empaneled vendor.

मधुकर कुमार भगत
संयुक्त सचिव
Madhukar Kumar Bhagat
Joint Secretary

सत्यमेव जयते

भारत सरकार
स्वास्थ्य एवं परिवार कल्याण मंत्रालय
निर्माण भवन, नई दिल्ली-110011
GOVERNMENT OF INDIA
MINISTRY OF HEALTH & FAMILY WELFARE
NIRMAN BHAWAN, NEW DELHI - 110011

No. M-11011/6/2015-eHealth
Dated : 07th July, 2025

Dear Colleagues

As you are aware that with the expansion of digital health services and systems across the country and growing reliance on technology, the risk of security breaches, such as unauthorized access, data disclosure, alterations, and potential destruction of critical information, poses a significant threat. Accordingly, comprehensive and robust information security measures are need of the hour to protect and ensure the data privacy and safety of health information.

2. In this connection, I would like to apprise that e-Health Division in MoHFW had, in consultation with NRCes and CDAC Pune, prepared draft Information Security Policy for Healthcare (Version 1.0) and security guidelines for Consultants and outsourced staff. These guidelines, after due approval of Secretary H&FW, are enclosed for ready reference and compliance.

3. I would like to request that suitable instructions be given to all concerned officers/stakeholders for the successful implementation of the guidelines/policy.

Yours sincerely,

Encls: as above.

(Madhukar Kumar Bhagat)

To,
1. All AS/JS/EA
2. CEO-NHA, DG (DGHS)

Copy To:
1) PSO to Secretary (Health)
2) Sr.PPS to JS eHealth

(Madhukar Kumar Bhagat)

Room No. 243-B, 'A' Wing, Nirman Bhavan, New Delhi-110011
Tel. : 011-23061066, Mob. : 9013850435; E-mail : madhukar.k.bhagat@gov.in

DDA AIIMS PATNA <dda@aiimspatna.org>

For engagement/appointment of Government counsel from the panel of Union of India for defending Court cases where Union of India is also a party along with an Autonomous Body - reg.

pmssysection iv <pmssysectioniv@gmail.com> Fri, Dec 5, 2025 at 11:06 AM
To: vc <vc@soa.ac.in>, Ashok Mahapatra <akmahapatra22000@gmail.com>, anitasaxena@hotmail.com, anitasaxena1956@gmail.com, tejaspatel@apexheart.in, dir.sgpgims@gmail.com, director@sgpgi.ac.in, drbkjain@sadgurutrust.org, raj bahadur <rajbahadur9@gmail.com>, mohalirsic@gmail.com, Maj Gen Tapan Saha <tapansaha7@gmail.com>, ANANT PANDHARE <apandhare1@gmail.com>, anantpandhare@hedgewar.org, drrvr@sankaraeye.com, Yk Gupta <yk.ykgupta@gmail.com>, "Dr.Hemant Kumar" <drhkumar.nephro@gmail.com>, neerja.bhatla07@gmail.com, vasanthapadma123@gmail.com, drmeshram@hotmail.com, nkarora@inclentrust.org, CS Narayanan <brigcsnarayanan@gmail.com>, titiyal@gmail.com, dr prashant lavania <dr.plavania@gmail.com>, bkssanjay@hotmail.com, Dr Pramod Garg <pgarg10@gmail.com>, pgarg@aiims.edu, Dharmendra Gangwar <dsgangwar@yahoo.com>, Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, madhabananda@gmail.com, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, drppjoshi@aiimsnagpur.edu.in, Executive Director Raebareli <edaiimsrbl@gmail.com>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, "Prof. Dr. D.K. Singh, Director" <director@aiimsbathinda.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, "Dr.Shakti kumar Gupta" <shakti810505@gmail.com>, AIIMS JAMMU <director@aiimsjammu.edu.in>, ed@aiimsrajkot.edu.in, edaiimsrajkot2020@gmail.com, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, sachimohanty@rediffmail.in, "Sharma, DN" <sharmadn@aiims.edu>
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, "Dy Director Administration AIIMS, Raebareli" <ddaaiimsrbl@gmail.com>, "Dr. Pradip Kumar" <kpradip10@gmail.com>, dda@aiimskalyani.edu.in, DDA AIIMS Gorakhpur <dda@aiimsgorakhpur.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, office aiimsdeoghar <office.aiimsdeoghar@gmail.com>, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, DDA AIIMS Bibinagar <dda@aiimsbibinagar.edu.in>, dda@aiimsbilaspur.edu.in, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, aps101982@rediffmail.com, dda aiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, dda@aiimsguwahati.ac.in, raj08642@gmail.com, Mukesh Kumar <mac.prasad@gmail.com>, ddaaiimsawantipora1@gmail.com, premprakash.bth@gov.in, manoj@ndma.gov.in, Suprava Poddar <sup15.81997@gov.in>

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officers of PMSSY-IV Section at - premprakash.bth@gov.in; manoj @ndma.gov.in; sup15.81997@gov.in;
Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

2 attachments

Letter (274).pdf
83K

InstructionsCourtCase (5).pdf
4810K

No.:C-18011/52/2025-PMSSY-IV (8366971)
Government of India
Ministry of Health and Family Welfare
(PMSSY - IV Section)
***

Nirman Bhawan, New Delhi
Dated: 05-12-2025

To

(i)The Presidents, All New AIIMS
(ii)The Executive Directors, All New AIIMS

Subject: For engagement/appointment of Government counsel from the panel of Union of India for defending Court cases where Union of India is also a party along with an Autonomous Body - reg.

Sir/Madam,

I am directed to refer to Department of Legal Affairs's OM No. J-12012/2/2017-Judicial dated 30.06.2017, MoH&FW Legal Cell's OM No. C-18017/22/2021-Legal Cell dated 17.12.2021 and this Division's letter No. C-18011/81/2024-PMSSY-IV dated 29.10.2024 (Copies enclosed) on the above subject and to say that the court cases wherein Union of India is also a party along with AIIMS, the same should be defended on behalf of both AIIMS as well as Union of India by the panel counsel engaged by the Department of Legal Affairs, Government of India only.

2. This has approval of Competent Authority.

Yours faithfully,

Digitally signed by
Prem Prakash
Date: 05-12-2025
10:33:54

(Prem Prakash)
Under Secretary to the Government of India

Encl: As above.

Copy to: The Dy. Directors (Admin), All New AIIMS

No.:C- 18011/81/2024-PMSSY-IV
Government of India
Ministry of Health and Family Welfare
(PMSSY - IV Section)
***

Room No:745A, Nirman Bhawan, New Delhi
Dated 29-10-2024

To

Executive Director, All New AIIMS

Subject: For engagement/appointment of Government counsel from the panel of Union of India for defending Court cases where Union of India is also a party along with an Autonomous Body - reg.

Sir,

I am directed to refer to Department of Legal Affairs's OM No. J-12012/2/2017-Judicial dated 30.06.2017 and MoHFW Legal Cell's OM No. C-18017/22/2021-Legal Cell dated 17.12.2021 on the above subject and to say that the court cases wherein Union of India is also a party along with AIIMS, the same should be defended on behalf of both, AIIMS as well as Union of India by the panel counsel engaged by the Department of Legal Affairs only.

Encl: As above

Yours faithfully,

Signed by Taranjeet Singh
Date: 29-10-2024 17:23:54

(Taranjeet Singh)
Under Secretary to the Government of India
Tel:011-23061343

Copy to:

Dy. Director (Admin), All New AIIMS

Gmail **pmssysection iv <pmssysectioniv@gmail.com>**

For engagement/appointment of Government counsel from the panel of Union of India for defending Court cases where Union of India is also a party along with an Autonomous Body - reg.

2 messages

pmssysection iv <pmssysectioniv@gmail.com> Mon, Nov 4, 2024 at 4:53 PM
To: Director AIIMS Bhopal <director@aiimsbhopal.edu.in>, director bhubaneswar <director@aiimsbhubaneswar.edu.in>, Director AIIMS Jodhpur <director@aiimsjodhpur.edu.in>, Director Patna <director@aiimspatna.org>, Director AIIMS Raipur <director@aiimsraipur.edu.in>, Director AIIMS Rishikesh <director@aiimsrishikesh.edu.in>, Director Mangalagiri <director@aiimsmangalagiri.edu.in>, Director AIIMS Nagpur <directoraiimsnagpur@gmail.com>, edaiimsrbl@gmail.com, rajwanshiarvind@hotmail.com, ED AIIMS Kalyani <ed@aiimskalyani.edu.in>, Executive Director Gorakhpur <executivedirector@aiimsgorakhpur.edu.in>, "Prof. Dr. D.K. Singh, Director" <director@aiimsbathinda.in>, Director AIIMS Deoghar <director@aiimsdeoghar.edu.in>, Bibinagar <director@aiimsbibinagar.edu.in>, Executive Director AIIMS BILASPUR <director@aiimsbilaspur.edu.in>, shakti810505@gmail.com, cdskatoch@gmail.com, Executive Director AIIMS Rajkot <ed.aiimsrajkot@gmail.com>, HanumanthaRao Mangu <drmhraosvims1957@gmail.com>, Director AIIMS Guwahati <director@aiimsguwahati.ac.in>, madhabananda@gmail.com, sachimohanty@rediffmail.in
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, DDA AIIMS JODHPUR <dda@aiimsjodhpur.edu.in>, DDA AIIMS PATNA <dda@aiimspatna.org>, DDA AIIMS Raipur <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, DDA@aiimsrbl.edu.in, "Dr. PRADIP KUMAR" <kpradip10@gmail.com>, dda@aiimskalyani.edu.in, dda@aiimsgorakhpur.edu.in, Rajeev Sen Roy <rajeevsenroy30@gmail.com>, Lt Col Rajeev Sen Roy <dda@aiimsbathinda.edu.in>, DDA Administration <dda@aiimsdeoghar.edu.in>, AMRENDRA KUMAR <amrendra.kumar72@gov.in>, office.aiimsdeoghar@gmail.com, dda aiimsbibinagar <dda.aiimsbibinagar@gmail.com>, dda@aiimsbibinagar.edu.in, ddaaiimsbilaspur <ddaaiimsbilaspur@gmail.com>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, Administrative Officer <ao.aiimsmadurai@gmail.com>, t.ngamlien@icg.gov.in, Mukesh Kumar <mac.prasad@gmail.com>, ddaaiimsawantipora1@gmail.com, "Cc:" <dinesh.kumar14@nic.in>, ":" <ak.biswas57@nic.in>, taranjeet.singh@nic.in, vaishali.vinayak@gov.in, sup15.81997@gov.in

Sir/ Madam

Please find the attachment.

Note: pmssysectioniv@gmail.com is an issue only email id. In case this email requires you to reply, you are requested to reply to all the officials of PMSSY-IV Section at - dinesh.kumar14@nic.in; ak.biswas57@nic.in; taranjeet.singh@nic.in; vaishali.vinayak@gov.in; sup15.81997@gov.in;
Regards
PMSSY-IV Section
Ministry of Health and Family Welfare

2 attachments

document - 2024-11-04 (2).pdf
50K

Encl (9).pdf
4629K

HanumanthaRao Mangu <drmhraosvims1957@gmail.com> Mon, Nov 4, 2024 at 4:52 PM

To: pmssysectioniv@gmail.com

F. No. J-12012/2/2017-Judicial
Government of India
Ministry of Law & Justice
Department of Legal Affairs
Judicial Section

Shastri Bhawan, New Delhi,
Date 29th June, 2017

OFFICE MEMORANDUM

Sub: ***For engagement / appointment of Government counsel from the panel of Union of India for defending Court cases where Union of India is also a party alongwith an Autonomous Body.***

The undersigned is directed to state that it has come to notice of this Department that in a number of cases before Tribunals and Courts, where Union of India and autonomous bodies are the main contestant parties, the Counsel appearing on behalf of autonomous bodies are not defending the cases in true spirit. This has resulted in matters having been lost despite the fact that experienced panel Counsel (for UoI) were available to properly defend the case.

2. Apart from the above, Ministry of Law & Justice has received complaints against the Counsel representing autonomous bodies that many such Counsel are not assisting the panel Counsel of Union of India wherever they have been engaged, giving way to many legal complications / problems due to the vested interests of such Counsel.

3. It is also pertinent to mention here that most of the autonomous bodies are not only funded by Government of India but also governed by various rules and regulations of the Government of India. They are also cooperative with the Government of India in implementing various policy decisions. Any adverse decision of the courts impacts the policy framework of the Government as well as set principals and also imposes huge financial implications on the Government of India.

4. In light of the above, all the Ministries / Departments are advised to issue instructions to the autonomous bodies under their administrative control that the cases where Union of India is also a party along with an autonomous body, should be defended on behalf of both, the autonomous body as well as Union of India before any Court / Tribunal by the panel Counsel engaged by the Department of Legal Affairs only.

This issues with the approval of competent authority.

(R. K. Srivastava)
Deputy Legal Adviser

All the Ministries / Departments of Govt. of India.

File No. C-18011/81/2024-PMSSY-IV (Computer No. 8298781)
Generated from eOffice by SARITA - EA(S) PMSSY, DEO, DOHFW, DEPARTMENT on 24/11/2024 04:39 pm

File No. C.18017/22/2021-Legal Cell
Government of India
Ministry of Health and Family welfare
Department of Health and Family Welfare

Nirman Bhawan New Delhi
Dated : 17/12/2021

OFFICE MEMORANDUM

Subject :- For engagement/ appointment of Government counsel from the panel of Union of India for defending court cases where Union of India is also a party alongwith an Autonomous Body.

The undersigned is directed to forward herewith D.O. Letter No. J-18/50/2021-Judicial dated 09.12.2021 from Secretary, Department of Legal Affairs and Office Memorandum J-12012/2/2017- Judicial dated 30.06.2017 (copy enclosed) on the above subject received from Department of Legal Affairs wherein the Ministries/Departments of Government of India have been advised to issue instructions to the autonomous bodies under their administrative control that the 1Court Cases wherein Union of India is also a party along with an autonomous body, the same should be defended on behalf of both, the autonomous body as well as Union of India by the Panel Counsel engaged by the Department of Legal Affairs only.

2. In this regard, all the autonomous bodies and the Divisions of the Ministry are requested to comply with the instructions as received from the Department of Legal Affairs in this regard.

This issues with the approval of Competent Authority.

Digitally Signed by Manish Raj
Date: 17-12-2021 14:44:41
Reason: Approved
(Manish Raj)

Under Secretary to the Government of India
email: legal-mohfw@gov.in
Telephone:011-23062068

Enclosure: As above

To,

1. The DGHS, Dte. General Health Services, Nirman Bhawan, New Delhi.
2. The Secretary, Deptt. of Health Research, IRCS Building, New Delhi.
3. Heads of all Autonomous Bodies under MoHFW.

File No. C-18011/81/2024-PMSSY-IV (Computer No. 8298781)
Generated from eOffice by SARITA, EA(S) PMSSY, DEO, DOHFW, DEPARTMENT on 04/11/2024 04:39 pm

भारत सरकार /Government of India
वित्त मंत्रालय /Ministry of Finance
व्यय विभाग/Department of Expenditure
ई III (क) शाखा/E.III(A) Branch
****

Ref: M/o Health & Family Welfare's eFile No. Z-28016/192/2020-PMSSY-IV-Part(1).

Ministry of Health & Family Welfare may refer to their e-file (Computer No.300615314) regarding implementation of technical resignation to the employees (faculty and non-faculty) in various New AIIMS set up under PMSSY.

2. The proposal has been considered in this Department. Ministry of Health & Family Welfare is advised to review the proposal in light of the following observations:-

(i) It is stated that AIIMS, New Delhi and 22 other new AIIMS are established under AIIMS Act, 1956 with AIIMS Amendment Act, 2012. However, the proposal has been moved only for the 22 new AIIMS excluding AIIMS, New Delhi. Whereas, IFD had concurred the proposal for extending this benefit to the employees of AIIMS, New Delhi.

It may be clarified whether the provision of technical resignation has already been extended to the employees of AIIMS, New Delhi and if so, whether the approval of this Department was sought in this regard. A clear view for extending the provision of technical resignation to AIIMS, New Delhi may be placed on file.

(ii) There appears to be large number of medical Autonomous Bodies under M/o H&FW other than AIIMS. The instant proposal has been covering the employees of AIIMS only. On extending the benefits of technical resignation exclusively to the employees of AIIMS, whether similar demands would not be raised by the other Autonomous Bodies under M/o H&FW.

(iii) The provisions for movement of employees other than resignation within AIIMS and other independent autonomous bodies may be clarified.

(iv) Although MoH&FW has attempted to confirm from M/o Education whether the provision of technical resignation is available to the employees of IITs / IIMS/ ABs under M/o Education. However, no reply has been received from M/o Education in this regard. It is advised to seek comments of M/o Education urgently in this regard.

(v) Retention of lien is the part of the provisions of technical resignation. Similarly, instructions of DOPT clearly provide that on technical resignation, seniority in the post held by the employee on substantive basis in parent cadre continue to be protected. Therefore, the proposal of MoHFW for non-retention of lien and not maintaining the seniority in the post held by the employee on substantive basis appears to be inconsistent with the policy of government in respect of Central Government servants.

3. This issues with the approval of the competent authority.

24/07/2024

(Vijay Kumar Sharma)
Under Secretary (E.III.A)

AS & FA, Ministry of Health & Family Welfare, Nirman Bhawan, New Delhi
Department of Expenditure, ID No. 14-04/2024-E.III.A, dated: 24.07.2024

File No. C-18011/81/2024-PMSSY-IV (Computer No. 8298781)
Generated from eOffice by SARITA, EA(S) PMSSY, DEO, DOHFW DEPARTMENT on 24/11/2024 01:10 pm

DDA AIIMS PATNA <dda@aiimspatna.org>

Preferential procurement of pharmaceutical products manufactured by Goa Antibiotics and Pharmaceuticals Limited (GAPL)-reg

3 messages

Mr Sourabh <pmssy5-mohfw@gov.in> Tue, Dec 9, 2025 at 3:18 PM
To: director <director@aiimsbhopal.edu.in>, director <director@aiimsbhubaneswar.edu.in>, director <director@aiimsjodhpur.edu.in>, director <director@aiimspatna.org>, director <director@aiimsraipur.edu.in>, director <director@aiimsrishikesh.edu.in>, edaiimsrbl <ed.aiimsrbl@gmail.com>, director <director@aiimsmangalagiri.edu.in>, directoraiimsnagpur <directoraiimsnagpur@gmail.com>, ed <ed@aiimskalyani.edu.in>, executivedirector <executivedirector@aiimsgorakhpur.edu.in>, director <director@aiimsbathinda.edu.in>, director <director@aiimsguwahati.ac.in>, executive-director <executive-director@aiimsguwahati.ac.in>, edaiimsbls <edaiimsbls@gmail.com>, director <director@aiimsbilaspur.edu.in>, director <director@aiimsdeoghar.edu.in>, rakeshkumar7123 <rakeshkumar7123@yahoo.in>, edaiimsrajkot <ed.aiimsrajkot@gmail.com>, directoraiimsbbnagar <director.aiimsbbnagar@gmail.com>, madhabananda <madhabananda@gmail.com>, drmhraosvims1957 <drmhraosvims1957@gmail.com>, shakti810505 <shakti810505@gmail.com>, director <director@aiimsjammu.edu.in>, sachimohanty <sachimohanty@rediffmail.in>
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, dda <dda@aiimsjodhpur.edu.in>, dda <dda@aiimspatna.org>, dda <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, ddaaiimsrbl <ddaaiimsrbl@gmail.com>, dda <dda@aiimsnagpur.edu.in>, kpradip10 <kpradip10@gmail.com>, dda <dda@aiimsgorakhpur.edu.in>, ashwanimahaur <ashwanimahaur@gmail.com>, rajeevsenroy30 <rajeevsenroy30@gmail.com>, ddaaiimsbilaspur <ddaaiimsbilaspur@gmail.com>, dda <dda@aiimsbilaspur.edu.in>, dda <dda@aiimsdeoghar.edu.in>, ddamadurai1189 <ddamadurai1189@gmail.com>, ddaaiimsrajkot <dda.aiimsrajkot@gmail.com>, ddaaiimsbibinagar <dda.aiimsbibinagar@gmail.com>, dda <dda@aiimsguwahati.ac.in>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, macprasad <mac.prasad@gmail.com>, ddaaiimsawantipora1 <ddaaiimsawantipora1@gmail.com>, dda <dda@aiimsmangalagiri.edu.in>, Aditya Kumar Mamgain <mamgain.aditya@lss.sansad.in>, Dharm SIngh <dharmbk.singh@nic.in>, Sourabh <sourabh.12@gov.in>, NARVEER REDHU <narveer.redhu@gov.in>

आदरणीय महोदय/महोदया,

उपर्युक्त विषय के संदर्भ में, कृपया संलग्न अनुलग्नक देखें।

सादर
पीएमएसएसवाई-V
निर्माण भवन
512-बी, ए विंग,
नई दिल्ली-110011

2 attachments

Ministries letter dated 09.12.2025.pdf
84K

HPE OM dated 18-11-2025.pdf
2872K

DDA AIIMS PATNA <dda@aiimspatna.org> Wed, Dec 10, 2025 at 11:02 AM
To: Amit Kumar Sinha <amit.sinha@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507
[Quoted text hidden]

2 attachments

Ministries letter dated 09.12.2025.pdf
84K

HPE OM dated 18-11-2025.pdf
2872K

Director . <director@aiimspatna.org> Wed, Dec 10, 2025 at 4:25 PM
To: DDA AIIMS PATNA <dda@aiimspatna.org>, medical superitendent <ms@aiimspatna.org>, MS Office <mso@aiimspatna.org>

Sd/-
Prof. (Brig.) Dr. Raju Agarwal
Executive Director
All India Institute of Medical Sciences Patna
Bihar - 801 507
Email: director@aiimspatna.org
Tel: 06122451109

---------- Forwarded message ---------
From: **Mr Sourabh** <pmssy5-mohfw@gov.in>
Date: Tue, Dec 9, 2025 at 3:20 PM
Subject: Preferential procurement of pharmaceutical products manufactured by Goa Antibiotics and Pharmaceuticals Limited (GAPL)-reg
To: director <director@aiimsbhopal.edu.in>, director <director@aiimsbhubaneswar.edu.in>, director <director@aiimsjodhpur.edu.in>, director <director@aiimspatna.org>, director <director@aiimsraipur.edu.in>, director <director@aiimsrishikesh.edu.in>, edaiimsrbl <ed.aiimsrbl@gmail.com>, director <director@aiimsmangalagiri.edu.in>, directoraiimsnagpur <directoraiimsnagpur@gmail.com>, ed <ed@aiimskalyani.edu.in>, executivedirector <executivedirector@aiimsgorakhpur.edu.in>, director <director@aiimsbathinda.edu.in>, director <director@aiimsguwahati.ac.in>, executive-director <executive-director@aiimsguwahati.ac.in>, edaiimsbls <edaiimsbls@gmail.com>, director <director@aiimsbilaspur.edu.in>, director <director@aiimsdeoghar.edu.in>, rakeshkumar7123 <rakeshkumar7123@yahoo.in>, edaiimsrajkot <ed.aiimsrajkot@gmail.com>, directoraiimsbbnagar <director.aiimsbbnagar@gmail.com>, madhabananda <madhabananda@gmail.com>, drmhraosvims1957 <drmhraosvims1957@gmail.com>, shakti810505 <shakti810505@gmail.com>, director <director@aiimsjammu.edu.in>, sachimohanty <sachimohanty@rediffmail.in>
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, dda <dda@aiimsjodhpur.edu.in>, dda <dda@aiimspatna.org>, dda <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, ddaaiimsrbl <ddaaiimsrbl@gmail.com>, dda <dda@aiimsnagpur.edu.in>, kpradip10 <kpradip10@gmail.com>, dda <dda@aiimsgorakhpur.edu.in>, ashwanimahaur <ashwanimahaur@gmail.com>, rajeevsenroy30 <rajeevsenroy30@gmail.com>, ddaaiimsbilaspur <ddaaiimsbilaspur@gmail.com>, dda <dda@aiimsbilaspur.edu.in>, dda <dda@aiimsdeoghar.edu.in>, ddamadurai1189 <ddamadurai1189@gmail.com>, ddaaiimsrajkot <dda.aiimsrajkot@gmail.com>, ddaaiimsbibinagar <dda.aiimsbibinagar@gmail.com>, dda <dda@aiimsguwahati.ac.in>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, macprasad <mac.prasad@gmail.com>, ddaaiimsawantipora1 <ddaaiimsawantipora1@gmail.com>, dda <dda@aiimsmangalagiri.edu.in>, Aditya Kumar Mamgain <mamgain.aditya@lss.sansad.in>, Dharm SIngh <dharmbk.singh@nic.in>, Sourabh <sourabh.12@gov.in>, NARVEER REDHU <narveer.redhu@gov.in>

[Quoted text hidden]

---

2 attachments

Ministries letter dated 09.12.2025.pdf
84K

HPE OM dated 18-11-2025.pdf
2872K

File No. Z-28016/161/2025(8376448)
Government of India
Ministry of Health & Family Welfare
Department of Health & Family Welfare
(PMSSY-V Section)

Nirman Bhawan, New Delhi-11
Dated:09-12-2025

To
The Executive Director,
All AIIMS under PMSSY.

Subject: Preferential procurement of pharmaceutical products manufactured by Goa Antibiotics and Pharmaceuticals Limited (GAPL)-reg.

Sir/Madam,

I am directed to refer to OM No. A-45013/63/2024-HPE dated November 18, 2025, received from the HPE Section, Ministry of Health & Family Welfare, regarding preferential procurement of pharmaceutical products manufactured by Goa Antibiotics and Pharmaceuticals Limited (GAPL) and to forward the same for necessary compliance .

2. This issues with the approval of Competent Authority.

Yours faithfully,

Digitally signed by
Dharm Bir Kumar Singh
Date: 09-12-2025
10:45:50

(Dharm Bir Kumar Singh)
Under Secretary to the Govt. of India
Tel: 011-23062319

Encl: as above

Copy to:

DDA, All AIIMS under PMSSY.

No. A-45013/63/2024-HPE
Government of India
Ministry of Health and Family Welfare
Department of Health & Family Welfare
(HPE Section)

Nirman Bhawan, New Delhi
Dated 18th November, 2025

OFFICE MEMORANDUM

Subject:Preferential procurement of pharmaceutical products manufactured by Goa Antibiotics and Pharmaceuticals Limited (GAPL) – reg.

The undersigned is directed to convey the approval of Department of Health and Family Welfare for the following:

CGHS and AIIMS shall procure, on a preferential basis, the 50 pharmaceutical items (out of total 104 PPP- listed products) for which GAPL holds valid manufacturing licenses. The complete list of products for which GAPL holds manufacturing licenses and which can be offered to CGHS and AIIMS is enclosed herewith at Annexure-I

2. This issues with the approval of Hon'ble HFM.

Encl.: As above.

Digitally signed by
SRIKANT SINGH KUSHWAHA
Date: 18-11-2025 12:09:58

(Srikant Singh Kushwaha)
Under Secretary to the Government of India
Tele : 011- 2306 3481

For circulation to all AIIMS/INIS for compliance
20/11/25

~~JD(AK)~~/Dir(INI)
DS(AKM)

To

1. JS (CGHS), DoHFW
2. JS(INI & PMSSY), DoHFW
3. JS(Hospital Division), DoHFW

JS(DBK)
Pl. circulate.
29/11/25

Copy for information to: Deputy Chief Executive Officer, GAPL, Goa.

- please circulate to all AIIMS under PMSSY

ASO(DK)

File No. Z-28016/161/2025-PMSSY-V (Computer No. 8376448)
Generated from eOffice by DHANANJAY KUMAR, ASO(DK) PMSSY-V MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 03/12/2025 04:34 pm

GAPL

ANNEXURE 1

LIST OF PRODUCTS THAT GAPL CAN MANUFACTURE

S.NO	NAME OF THE PRODUCT
1	Aceclofenac and Paracetamol Tablet 100mg + 325mg
2	Albendazole Tablet I.P. 400 mg
3	Alcoholic Hand Disinfectant Solution
4	Amlodipine Tablet I.P. 5 mg
5	Amoxycillin and Potassium Clavulanate Tablet I.P. 500mg + 125mg
6	Amoxycillin Capsule I.P. 250 mg
7	Amoxycillin Capsule I.P. 500 mg
8	Amoxycillin Oral Suspension I.P. 125mg/5mL
9	Ascorbic Acid Tablet I.P. 500 mg
10	Atorvastatin Tablet 20 mg
11	Atorvastatin Tablet I.P. 10 mg
12	Azithromycin Tablet I.P. 250 mg
13	Azithromycin Tablet I.P. 500 mg
14	Calcium Carbonate and Vit D3 Capsule 500mg + 250iu
15	Cefixime Tablet I.P. 100 mg
16	Cefixime Tablet I.P. 200 mg
17	Cefoperazone and Sulbactam Injection 1G + 1G
18	Ceftriaxone Injection I.P. 1 G
19	Cefuroxime Axetil Tablet I.P. 250 mg
20	Cefuroxime Axetil Tablet I.P. 500 mg
21	Cetirizine Syrup 5mg/5mL
22	Cetirizine Tablet I.P. 10 mg
23	Ciprofloxacin and Tinidazole Tablet 500mg + 600mg
24	Ciprofloxacin Tablet I.P. 500 mg
25	Clotrimazole Cream I.P. 1% W/W

Sijo Joy Edapully
Dy. Chief Executive Officer
Goa Antibiotics & Pharmaceuticals Ltd.
(A Government of India Enterprise)
Tuem, Pernem - Goa 403512.

गोवा एंटीबायोटिक्स एंड फार्मास्युटिकल्स लिमिटेड

Goa Antibiotics & Pharmaceuticals Ltd.
(Subsidiary of HLL Lifecare Ltd.
A Government of India Enterprise)
Near Tuem Industrial Estate
Goa 403 512, India
Tel: +91 832 2301 417

File No. Z-28016/161/2025-PMSSY-V (Computer No. 8376448)
Generated from eOffice by DHANANJAY KUMAR - ASO(DK) PMSSY V MOHFW - ASSISTANT SECTION OFFICER - DOHFW DEPARTMENT on 03/12/2025 01:24 pm

ANNEXURE 1

LIST OF PRODUCTS THAT GAPL CAN MANUFACTURE

26	Cough Syrup -Each 5ML Contains Diphenhydramine Hydrochloride IP 14 MG Sodium Citrate IP 57 MG Menthol IP 0.9 Mg
27	Diclofenac and Paracetamol Tablet 50mg + 325mg
28	Diclofenac Ointment 1% w/v
29	Dicyclomine and Paracetamol Tablet 20mg + 500mg
30	Doxycycline Capsule I.P. 100 mg
31	Ethyl Alcohol Solution 70% Alcoholic Hand Disinfectant Bottle of 500ml
32	Fluconazole Tablet I.P. 150 mg
33	Glimepiride Tablet I.P. 1 mg
34	Glimepiride Tablet I.P. 2 mg
35	Ibuprofen and Paracetamol Tablet 400mg + 325mg
36	Inj Ceftriaxone 1g and Sulbactum 500mg Injection
37	Levocetirizine Tablet I.P. 5 mg
38	Levofloxacin Tablet 500 mg
39	Losartan Tablet I.P. 50 mg
40	Metformin Tablet I.P. 500 mg
41	Metronidazole Tablet I.P. 400 mg
42	Norfloxacin and Tinidazole Tablet 400mg plus 600mg
43	Ofloxacin and Ornidazole Tablet 200mg + 500mg
44	Omeprazole 20mg and Domperidone 10mg Capsule
45	Omeprazole Capsule I.P. 20 mg
46	Oral Rehydration Salts Containing Detrose (Anhydrous), Sodium Chloride, Potassium Chloride and Sodium Citrate Sachet I.P 13.5 G/L + 2.6 G/L + 1.5 G/L + 2.9 G/L Powder for Dilution In 200Ml; 500 Ml, 1000Ml.
47	Pantoprazole Enteric Coated Tablet 40 mg
48	Paracetamol Syrup I.P. 125mg/5mL
49	Paracetamol Tablet 650 mg
50	Paracetamol Tablet I.P. 500 mg

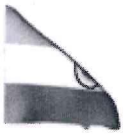
Sijo Joy Edapully
Dy. Chief Executive Officer
Goa Antibiotics & Pharmaceuticals Ltd.
(A Government of India Enterprise)
Tuem, Pernem - Goa 403512.

File No. A-45013/63/2024-HPE (Computer No. 8298566)
File No. Z-28016/16/2025-PMSSY-I (Computer No. 8376448)
Generated from eOffice by DHANANJAY KUMAR, ASO(DK), PMSSY-V MOHFW, ASSISTANT SECTION OFFICER, DOHFW DEPARTMENT on 12/09/2025 04:24 pm

DDA AIIMS PATNA <dda@aiimspatna.org>

Compliance of stringent and time-bound directions of Hon'ble Supreme Court of India to all States/UTs and the Union of India regarding a significant rise in dog-bite incidents in institutional spaces.

Vijay Kumar Gupta <vijaykr.gupta@nic.in> Tue, Dec 9, 2025 at 6:15 PM
To: director <director@aiimsawantipora.edu.in>, ed <ed@aiimsrajkot.edu.in>, edaiimsrajkot2020 <edaiimsrajkot2020@gmail.com>, director <director@aiimsbhopal.edu.in>, director <director@aiimsbhubaneswar.edu.in>, director <director@aiimsjodhpur.edu.in>, director <director@aiimspatna.org>, director <director@aiimsraipur.edu.in>, director <director@aiimsrishikesh.edu.in>, director <director@aiimsmangalagiri.edu.in>, directoraiimsnagpur <directoraiimsnagpur@gmail.com>, drppjoshi <drppjoshi@aiimsnagpur.edu.in>, edaiimsrbl <edaiimsrbl@gmail.com>, executivedirector <executivedirector@aiimsgorakhpur.edu.in>, ed <ed@aiimskalyani.edu.in>, director <director@aiimsdeoghar.edu.in>, director <director@aiimsbibinagar.edu.in>, director <director@aiimsbilaspur.edu.in>, sharmadn <sharmadn@aiims.edu>, shakti810505 <shakti810505@gmail.com>, director <director@aiimsjammu.edu.in>, drmhraosvims1957 <drmhraosvims1957@gmail.com>, director <director@aiimsguwahati.ac.in>, madhabananda <madhabananda@gmail.com>, sachimohanty <sachimohanty@rediffmail.in>, dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, dda <dda@aiimsjodhpur.edu.in>, dda <dda@aiimspatna.org>, dda <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, rajeevsenroy30 <rajeevsenroy30@gmail.com>, dda <dda@aiimsbathinda.edu.in>, dda <dda@aiimsmangalagiri.edu.in>, ddaiimsnagpur1 <ddaiimsnagpur1@gmail.com>, dda <dda@aiimsrbl.edu.in>, ddaaiimsrbl <ddaaiimsrbl@gmail.com>, kpradip10 <kpradip10@gmail.com>, dda <dda@aiimskalyani.edu.in>, dda <dda@aiimsgorakhpur.edu.in>, dda <dda@aiimsdeoghar.edu.in>, officeaiimsdeoghar <office.aiimsdeoghar@gmail.com>, ddaaiimsbibinagar <dda.aiimsbibinagar@gmail.com>, dda <dda@aiimsbibinagar.edu.in>, dda <dda@aiimsbilaspur.edu.in>, macprasad <mac.prasad@gmail.com>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, aps101982 <aps101982@rediffmail.com>, ddaaiimsrajkot <dda.aiimsrajkot@gmail.com>, ddamadurai1189 <ddamadurai1189@gmail.com>, aoaiimsmadurai <ao.aiimsmadurai@gmail.com>, dda <dda@aiimsguwahati.ac.in>, deputydirector <deputydirector@aiimsawantipora.edu.in>
Cc: kumarakhilesh <kumar.akhilesh@gov.in>, ravikumar89 <ravi.kumar89@gov.in>, vikaskumar76 <vikas.kumar76@gov.in>, arvindthakur <arvind.thakur@nic.in>, Shalaka Kujur <shalaka.kujur@nic.in>, mamgainaditya <mamgain.aditya@gov.in>



Sir/Madam,

Kindly find attached herewith communications on the subject mentioned above for necessary action.

सादर धन्यवाद/Regards,

विजय कुमार गुप्ता / Vijay Kumar Gupta,

अवर सचिव / Under Secretary,

स्वास्थ्य एवं परिवार कल्याण विभाग / Department of Health & Family Welfare,

कमरा न. 745A/ Room No. 745A,

निर्माण भवन/Nirman Bhawan,

नई दिल्ली 110 011 / New Delhi 110 011.

Phone # 011-23061343

2 attachments

OM dated 03.12.25 regarding directives of Honble Supreme Court.pdf
24921K

OM dated 09.12.25.pdf
63K

Z.21020/242/2025-PH

(Comp. No. 8374321)

Government of India

Ministry of Health and Family Welfare

Department of Health and Family Welfare

Public Health Division

Nirman Bhawan, New Delhi

Dated 03 December, 2025

OFFICE MEMORANDUM

Subject: Compliance with the directions of the Hon'ble Supreme Court in Suo Moto W.P. (C) No. 5/2025 titled *"IN RE: CITY HOUNDED BY STRAYS, KIDS PAY PRICE"* – reg.

The undersigned is directed to refer to D.O. letter of even number dated 2nd December 2025 from Secretary (HFW) to all Secretaries of Government of India and all Chief Secretaries of States/ UTs on the subject cited above and to say that the Supreme Court, noting a significant rise in dog-bite incidents in institutional spaces, has issued stringent and time-bound directions to all States/UTs and the Union of India to secure educational institutions, hospitals, sports complexes, bus stands/depots and railway stations from stray-dog ingress vide order dated 07.11.2025 in the **Suo Moto W.P. (c) No. 5/25 "CITY HOUNDED BY STRAYS, KIDS PAY PRICE"** pending before the Hon'ble Supreme court of India.

2. The major Directives (Part IV) in the order dt. 07-11-2025 are:

i. Identification & Securing of Premises within two weeks every Government and private educational institution (schools, colleges, hostels), hospital and medical facility, sports complex/stadium, bus stand/ISBT, railway station and **secure them** through fencing, boundary walls, gates and similar structural/administrative measures **within eight weeks**.

ii. Each institution must designate a **Nodal Officer** responsible for cleanliness, preventing dog ingress, liaison with municipal authorities and display the details of the Nodal Officer prominently and notified to the municipal body.

iii. Mandated **Quarterly inspections** to ensure no dog habitats exist within or near these premises. Immediately remove any stray dog found inside the institution and sterilised and vaccinated, and **not returned to the same location**.

iv. All Government and private hospitals must **maintain mandatory stock of anti-rabies vaccine (ARV) and immunoglobulin (RIG)** at all times.

v. **Complaince affidavits to be filed within 8 weeks** by **Chief Secretaries** of all States/UTs, **NHAI, Union of India (MoHFW)** covering securing of Central Government institutions, coordination mechanisms, availability of ARV/RIG, and compliance with ABC Rules, 2023.

3. As per the Supreme Court Directive MoHFW is required to file a comprehensive compliance affidavit within eight weeks. The court directive is reproduced hereuner:

"The Union of India, through the Ministry of Health and Family Welfare, shall file a comprehensive affidavit of compliance within a period of 8 weeks from today (07-11-2025), indicating the steps taken to secure such institutions, the mechanism evolved for coordination with local/municipal authorities, and the measures adopted for ensuring the availability of

770

Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

anti-rabies vaccines and immunoglobulin in Central Government hospitals and healthcare facilities."

4. All the divisions are therefore requested to take necessary action as per the court directive and submit a compliance report to PH Division by 19-12-2025 to enable filling a comprehensive compliance affidavit in the Supreme Court.

5. It is requested to **closely monitor and ensure timely compliance** by institutions under the administrative control and furnish a **comprehensive status report to this division within 4 weeks**, to facilitate filing of the compliance affidavit before the Hon'ble Supreme Court on behalf of the Union of India.

6. The **DS/Directors of the respective Divisions have been designated as the Nodal Officer** to gather the relevant information pertaining to matters arising out of the above-mentioned directions of the Hon'ble Supreme Court.

7. This issues with the approval of the competent authority.

Encl.: As above

Walia

(Jasminder Ahluwalia)
Under Secretary to the Government of India
Tel.: 011-23062032

To:

1. All Director/ DS,
Ministry of Health & Family Welfare

2. DGHS

3. DHR

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)
Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

पुण्य सलिला श्रीवास्तव, भा.प्र.से.
सचिव
PUNYA SALILA SRIVASTAVA, IAS
Secretary

सत्यमेव जयते

भारत सरकार
स्वास्थ्य एवं परिवार कल्याण विभाग
स्वास्थ्य एवं परिवार कल्याण मंत्रालय
Government of India
Department of Health and Family Welfare
Ministry of Health and Family Welfare

D.O.No.Z.21020/242/2025-PH
2nd December, 2025

Dear Colleague,

This is to bring to your kind attention that the Hon'ble Supreme Court of India, noting a significant rise in dog-bite incidents in institutional areas, has issued stringent and time-bound directions to all States/UTs and the Union of India to secure educational institutions, hospitals, sports complexes, bus stands/depots and railway stations from stray-dog ingress vide Order dated 07.11.2025 in **Suo Moto Writ Petition (Civil) No. 5 of 2025 IN RE: "CITY HOUNDED BY STRAYS, KIDS PAY PRICE"**. Copy of the Order is enclosed.

2. In accordance with aforesaid directions, following actions are required to be undertaken by Union of India, inter-alia, as per paras of the court order given below:

*"25C. The management of every educational institution, hospital, sports complex, bus stand/depot,(including Inter-State Bus Terminal) and railway, station identified under **Direction (A)** shall designate a Nodal Officer responsible for the upkeep and cleanliness of the premises and for ensuring that stray dogs do not enter or inhabit the campus. The details of the said officer shall be displayed prominently at the entrance and notified to the jurisdictional municipal body/authority.*

*25F. **All Government and private hospitals shall maintain a mandatory stock of anti-rabies vaccines and immunoglobulin at all times**.*

25 G. Every school and educational institution shall be directed by the Ministry of Education, Government of India, to conduct awareness sessions for students and staff on preventive behaviour around animals, first-aid in case of bites, and immediate reporting protocols.

25 H. The management of stadiums and sports complexes shall ensure the deployment of security or ground-keeping personnel specifically tasked with around the clock vigil against the entry or habitation of stray dogs.

25 I. The railway authorities having jurisdiction over the railway stations as well as the State transport corporations and municipal authorities having jurisdiction over bus stands, depots and Inter-State Bus Terminals, shall ensure that such public-transport premises/facilities are effectively secured and maintained so as to prevent the habitation or movement of stray dogs within their premises. Proper waste-management systems shall be implemented to eliminate food sources that attract animals, and regular inspections shall be conducted to detect and address the presence of stray dogs.

....contd/-

Room No. 11102, 'C' Wing, Kartavya Bhawan-1, New Delhi-110001
Tele: (O) 011-24013601, 24013602, E-mail: secyhfw@nic.in

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)
Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

25 J. Animal Welfare Board of India shall, within four weeks, issue detailed Standard Operating Procedures (SOPs) for prevention of dog bites and management of stray dogs in institutional premises (public or private) including but not limited to Government and private educational institutions, hospitals (including district hospitals, primary health centres, and medical colleges), and sports complexes or stadia, to be uniformly adopted across all States and Union Territories."

3. In this connection, I would request you to **ensure timely compliance of the court order** and furnish a **comprehensive report to the Ministry of Health & Family Welfare by 12th December, 2025**, to facilitate filing of the compliance affidavit by 6th Jan2025 before the Hon'ble Supreme Court on behalf of the Union of India.

4. I shall be grateful if you could kindly intervene personally and furnish the status report. Details of the appointed nodal officers, not below the rank of Joint Secretary, may also be shared.

5. The nodal officers from MoHFW would be Ms. Vandana Jain, Joint Secretary (Tel. No.011-23062699), email vandana.jain@nic.in) and Ms. G. S. Chitra, Director (Public Health) (Tel. No. 011-23061281; Email: gs.chitra@nic.in).

With regards,

Yours sincerely,

Punya Salila

Encl : as above

(Punya Salila Srivastava)

Secretary to Govt. of India
All Ministries / Departments

773

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)
Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

SPEED POST / OUT TODAY

D.NO. 41706/2025/SC/PIL (W)

All Communications should be addressed to the Registrar, Supreme Court by designation, NOT by name

SUPREME COURT
INDIA
NEW DELHI

Dated: 12th November, 2025

FROM : Assistant Registrar, PIL (WRIT)

4576998
14/11/2025

TO,

1 Ministry of Health and Family Welfare,
Through its Secretary,
Nirman Bhawan, New Delhi – 110011

2 Ministry of Education,
Through its Secretary,
Shastri Bhawan New Delhi – 110001

3 Ministry of Fisheries, Animal Husbandry and Dairying,
Through its Secretary,Krishi Bhawan,
New Delhi – 110001

4 Ministry of Youth Affairs and Sports,
Through its Secretary, C-Wing,
Shastri Bhawan New Delhi – 110001

5 Ministry of Road Transport and Highways,
Through its Secretary,
Transport Bhawan, 1, Parliament Street
New Delhi-110001

6 Ministry of Railways,
Through its Secretary,
256-A, Raisina Road, Rajpath Area,
Central Secretariat, New Delhi, 110001

7 Ministry of Panchayati Raj,
Through its Secretary,
11th Floor, Jeevan Prakash Building,
25 K.G.Marg, New Delhi-110001

8 Ministry of Rural Development,
Through its Secretary, Krishi Bhavan,
Dr. Rajendra Prasad Road,
New Delhi - 110001

9 National Highways Authority of India,
Through its Chairman,
G 5&6, Sector 10, Dwarka, New Delhi 110075

10 Animal Welfare Board of India,
Through its Secretary,
42 KM Stone, Delhi-Agra Highway,
National Highway-2, Village-Seekri, Ballabhgarh,
Faridabad, Haryana -121 004 India.

11 State of Andhra Pradesh,
Through the Chief Secretary,
Secretariat, Velagapudi
Andhra Pradesh

12 State of Arunachal Pradesh,
Through the Chief Secretary,
Secretariat, Itanagar
Arunachal Pradesh

13 State of Assam,
Through the Chief Secretary,
Secretariat, Guwahati
Assam

14 State of Bihar,
Through the Chief Secretary,
Secretariat, Patna
Bihar

15 State of Chhattisgarh,
Through the Chief Secretary,
Secretariat Mahanadi Bhawan
Naya Raipur,
Chhattisgarh

16 State of Goa,
Through the Chief Secretary,
Secretariat, Porvorim
Goa

17 State of Gujarat,
Through the Chief Secretary,
Secretariat, Gandhinagar
Gujarat

18 State of Haryana,
Through the Chief Secretary,
Secretariat, Chandigarh,
Haryana

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)
Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

19 State of Himachal Pradesh,
Through the Chief Secretary,
Secretariat, Shimla
Himachal Pradesh

20 State of Jharkhand,
Through the Chief Secretary,
Secretariat, Ranchi
Jharkhand

21 State of Karnataka,
Through the Chief Secretary,
Secretariat, Bangalore
Karnataka

22 State of Kerala,
Through the Chief Secretary,
Secretariat, Thiruvananthapuram
Kerala

23 State of Madhya Pradesh,
Through the Chief Secretary,
Secretariat, Bhopal,
Madhya Pradesh

24 State of Maharashtra,
Through the Chief Secretary,
Secretariat, Mantralaya,
Mumbai, Maharashtra

25 State of Manipur
Through the Chief Secretary,
Secretariat, Imphal
Manipur

26 State of Meghalaya,
Through the Chief Secretary,
Secretariat, Shillong
Meghalaya

27 State of Mizoram,
Through the Chief Secretary,
Secretariat, Aizawl,Mizoram

28 State of Nagaland,
Through the Chief Secretary,
Secretariat, Kohima
Nagaland

776

Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

29 State of Odisha,
Through the Chief Secretary,
Secretariat, Bhubaneshwar
Odisha

30 State of Punjab,
Through the Chief Secretary,
Secretariat,
Chandigarh

31 State of Rajasthan,
Through the Chief Secretary,
Secretariat, Jaipur,
Rajasthan

32 State of Sikkim,
Through the Chief Secretary,
Secretariat, Gangtok
Sikkim

33 State of Tamil Nadu,
Through the Chief Secretary,
Secretariat, Chennai,
Tamil Nadu

34 State of Telangana
Through the Chief Secreary,
Secretariat, Hyderabad
Telangana

35 State of Tripura,
Through the Chief Secretary,
New Secretariat Complex, Agartala
Tripura

36 State of Uttrakhand
Through the Chief Secretary,
Secretariat, Dehradun
Uttarakhand.

37 State of Uttar Pradesh
Through the Chief Secretary,
Secretariat, Lucknow
Uttar Pradesh

38 State of West Bengal,
Through the Chief Secretary,
Secretariat Headquarter

777

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)
Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

"Nabanna" HRBC Building, 325, Sarat Chatterjee Road,
Howrah -711 102, West Bengal

39 Union Territory of Andaman & Nicobar,
Through the Chief Secretary,
Secretariat,
Port Blair

40 Union Territory of Chandigarh,
Through the Chief Secretary,
Secretariat
Chandigarh-160001

41 Union Territory of Dadra & Nagar Haveli
and Daman & Diu
Through the Secretary
Secretariat, Fort Area
Moti Daman - 396220

42 Union Territory of National Capital Territory of Delhi
Through the Chief Secretary
Secretariat, I P Estate
New Delhi

43 Union Territory of Lakshadweep,
Through the Chief Secretary,
Secretariat,
Kavaratti- 682555

44 Union Territory of Puducherry
Through the Chief Secretary,
Secretariat
Puducherry- 605001

45 UT of Jammu & Kashmir,
Through Chief Secretary
Secretariat, Srinagar – 190001

46 UT of Ladakh
Through Lieutenant Governor
Civil Secretariat
Leh-Ladakh 194101

SUO MOTO WRIT PETITION (C) NO. 5 OF 2025

WITH
SLP(CIVIL) NO(S). 14763 OF 2024
SLP(CIVIL) NO(S). 17623 OF 2025
WRIT PETITION(CIVIL) NO(S). 784 OF 2025

SLP(CIVIL) NO(S). OF 2025 (Diary No. 45707 OF 2025)
T.C. (CIVIL) NO. 140 OF 2025
AND
CONTEMPT PETITION (C) NO(S). 749 OF 2025 IN SLP(CIVIL) NO(S). 14763 OF 2024

IN THE MATTER OF :-
IN RE: "CITY HOUNDED BY STRAYS, KIDS PAY PRICE"

vs

STATE OF ANDHRA PRADESH AND ORS.

Sir,

I am directed to forward herewith a certified copy of Signed Order dated 07.11.2025 passed in the matter above-mentioned along with Schedule I for your information, compliance and necessary action.

Please acknowledge receipt.

Yours faithfully,

12.11.25
Assistant Registrar

Certified to be true copy
Assistant Registrar (Judl.)
Supreme Court of India

REPORTABLE

IN THE SUPREME COURT OF INDIA
INHERENT/CIVIL ORIGINAL/
EXTRAORDINARY APPELLATE JURISDICTION

SUO MOTO WRIT PETITION(CIVIL) NO(S). 5 OF 2025

IN RE: "CITY HOUNDED BY STRAYS, KIDS PAY PRICE"

25152596

WITH

SLP(CIVIL) NO(S). 14763 OF 2024

SLP(CIVIL) NO(S). 17623 OF 2025

WRIT PETITION(CIVIL) NO(S). 784 OF 2025

SLP(CIVIL) NO(S). OF 2025
(Diary No. 45707 OF 2025)

T.C. (CIVIL) NO. 140 OF 2025

CONTEMPT PETITION (C) NO(S). 749 OF 2025 IN
SLP(CIVIL) NO(S). 14763 OF 2024

O R D E R

Mehta, J.

1. This Court, *vide* order dated 22nd August, 2025, after considering the submissions made on behalf of the parties and the material placed on record, had

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)
Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

supplemented, modified, and clarified the earlier directions issued *vide* order dated 11th August, 2025.

2. The directions contained in the order dated 22nd August, 2025, *inter alia*, mandated the municipal authorities to continue the exercise of capturing, sterilising, deworming, and vaccinating stray dogs in accordance with the Animal Birth Control Rules, 2023, while permitting the release of sterilised and immunised dogs to the same localities from which they were picked up, except those infected with or suspected to be infected with rabies and those exhibiting aggressive behaviour. The Court further directed the creation of designated feeding zones for stray dogs, establishment of municipal helplines for reporting violations, and the filing of comprehensive compliance affidavits by the respective municipal authorities.

3. The aforesaid directions were extended to all States and Union Territories, and the Registry was directed to seek information from the Registrar Generals of the High Courts with respect to similar matters pending before them, so that a uniform and

coherent approach to the menace of stray dogs could be evolved across the country.

4. The present order shall address three distinct issues, which are being dealt with in separate parts for clarity and convenience. **Part I** pertains to the compliance affidavits filed by the States and Union Territories pursuant to this Court's earlier directions and the summary report prepared by the learned Amicus Curiae, Shri Gaurav Agrawal. **Part II** concerns the modification, application and implementation of the directions issued by the High Court of Judicature for Rajasthan at Jodhpur in D.B. Civil Writ Petition No. 14726 of 2025. **Part III** concerns the issuance of further directions in respect of institutional areas, including educational establishments, hospitals, sports complexes, and other public spaces such as railway stations and bus depots, where incidents of dog-bite attacks continue to be reported with alarming frequency, raising a cause of grave concern and requiring emergent remedial measures.

PART I: Compliance Affidavits filed by States and UTs and Summary prepared by *Amicus Curiae*

5. Pursuant to the direction contained in paragraph 33(i) of the order dated 22nd August, 2025 and the subsequent order dated 27th October, 2025, all States and all Union Territories, except the Union Territory of Dadra and Nagar Haveli and Daman & Diu, have submitted their respective compliance affidavits before this Court. The learned *amicus curiae*, Shri Gaurav Agrawal, has been requested *vide* order dated 3rd November, 2025, to examine the said affidavits and to place before this Court a concise summary of the affidavits filed by the States and Union Territories in purported compliance with the directions issued by this Court.

6. In compliance of the order dated 3rd November, 2025, the learned *amicus curiae*, Shri Gaurav Agrawal, has made a herculean effort and has filed a report summarising the compliance affidavits submitted by the respective States and Union Territories. The report highlights several grave deficiencies and shortcomings in the information furnished by certain States and Union Territories, as

well as areas where compliance with the directions issued by this Court has either not been effected or remains incomplete. The learned *amicus curiae* has also tendered constructive suggestions and recommendations to ensure effective and uniform implementation of this Court's orders across jurisdictions.

7. The report submitted by the learned Amicus Curiae, Shri Gaurav Agrawal, is taken on record and shall form part of this Order. The Registry is directed to annex the same as **Schedule I**. The contents of the said report shall be read as part and parcel of this order for all purposes. The States and Union Territories shall peruse the report and take appropriate steps to address the deficiencies and shortcomings pointed out therein. Each State and Union Territory shall file comprehensive additional affidavits before the next date of hearing, specifically indicating the remedial measures undertaken to ensure full compliance with this Court's directions and to rectify the lapses highlighted in the report of the learned *amicus curiae*. Any lethargy in this regard shall be viewed seriously.

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)

11

784

Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

PART II: Modification, Application and Implementation of the Directions issued by High Court of for Rajasthan at Jodhpur in D.B. Civil Writ Petition No. 14726 of 2025.

8. It is a matter of grave and continuing public concern that accidents caused by cattle and other stray animals on public roads and highways have become alarmingly frequent across the country. Such incidents, often resulting in loss of human life, grievous injuries, and damage to property, are not isolated events but symptomatic of a larger failure on the part of the administrative authorities entrusted with public safety. The uncontrolled presence of cattle and stray animals on National Highways, National Expressways, and State Highways, constitutes a serious and avoidable threat, particularly during night-time or in high-speed zones.

9. This Court cannot remain unmindful of the preventable nature of these accidents, which not only reflect administrative indifference but also undermine the constitutional guarantee of the right to life and safety under Article 21. The need for immediate, coordinated, and sustained action by all

concerned agencies, i.e., municipal authorities, road and transport departments, public works departments and highway authorities, cannot be overstated.

10. Accordingly, this Court issues the following directions:

A. The directions issued by the **High Court of Rajasthan at Jodhpur in D.B. Civil Writ Petition No. 14726 of 2025 *vide* order dated 11th August, 2025,** are hereby reaffirmed, to the extent that the municipal authorities, road and transport department/Public Works Department of all the States and Union Territories and the National Highways Authority of India (NHAI) shall ensure the removal of all cattle and other stray animals from the State Highways, National Highways, and National Expressways falling within their respective jurisdictions.

B. The concerned authorities, i.e., the municipal authorities, the road and transport department/Public Works Department of all the States and Union Territories and the National Highways Authority of India shall undertake a joint, coordinated drive to identify stretches of

786

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)
Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

highways and expressways where stray cattle or animals are frequently found, and shall take immediate steps for their removal and relocation to designated shelters. The cattle and other stray animals so picked up shall be kept in appropriate shelters or *Gaushalas*/cattle pounds, as the case may be, and provided with all necessary food, water, and veterinary care, in accordance with the provisions of the Prevention of Cruelty to Animals Act, 1960 and the Animal Birth Control (Dogs) Rules, 2023.

C. Each authority shall constitute dedicated highway patrol teams and/or assign existing road-safety units for continuous surveillance and immediate response to reports of stray cattle or other animals obstructing the roadways. Such patrols shall function on a 24x7 basis and coordinate with local police stations, veterinary officers, and municipal authorities/Panchayati Raj institutions.

D. All National Highways, State Highways, and National Expressways shall have prominently displayed helpline numbers at regular intervals, enabling commuters to promptly report the presence of stray animals or accidents caused

787

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)
Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

thereby. These helplines shall be linked to the control rooms of the local police, National Highways Authority of India, and district administration for real-time redressal and monitoring.

E. The Chief Secretaries of all States and Union Territories, together with the Chairperson, National Highways Authority of India, shall ensure strict enforcement of these directions through appropriate administrative orders and field-level monitoring. They shall hold the concerned officers personally accountable for lapses or recurring incidents in their respective jurisdictions.

F. The aforesaid directions shall be implemented uniformly across India, and the Chief Secretaries of all States and Union Territories; Chairperson, National Highways Authority of India; and Ministry of Road Transport and Highways, Union of India shall file status-cum-compliance affidavits within a period of eight weeks from today, indicating:

i. the mechanism established for removal and sheltering of stray animals from highways;

ii. the constitution and functioning of patrol teams; and

iii. the operational status of helpline facilities and installation of sign boards displaying helpline numbers.

11. The Registry shall forthwith implead the National Highways Authority of India through its Chairperson.

PART III: Directions regarding Institutional Areas, i.e., educational institutions, hospitals, sports complexes, bus stands/depots and railway stations

12. In the interregnum, this Court has been apprised through various news reports and media accounts of disturbing increase in dog-bite incidents within the premises of educational institutions, hospitals, sports complexes, bus stands/depots (including Inter-State Bus Terminals) and railway stations, generically speaking, institutional areas. Instances of children being attacked in school campuses, patients and attendants being bitten within hospital compounds, athletes as well as officials being attacked by stray dogs inside sports stadiums and passengers/travellers being attacked

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)
Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

by stray dogs at bus stands/depots and railway stations, have come to the notice of this Court.

13. The recurrence of such incidents, particularly within institutional spaces meant for learning, healing, and recreation, reflects not only administrative apathy but also a systemic failure to secure these premises from preventable hazards. The situation calls for immediate judicial intervention to safeguard the fundamental right to life and safety of citizens, especially children, patients, and sportspersons, under Article 21 of the Constitution of India.

14. After Independence, despite significant advances in public health, India continues to report one of the world's highest statistics of rabies-related mortality. Scientific assessments, including those conducted by the World Health Organization (WHO) and the National Centre for Disease Control (NCDC), have estimated that a large ratio of animal related deaths annually in India were attributable to rabies, with over 90% of human cases resulting from bites inflicted by domestic or stray dogs. The brunt of this menace has been borne by children, elderly people

and economically weaker sections who in addition of being vulnerable, also lack timely access to post-exposure prophylaxis.

15. Recognising the need for a humane yet effective framework, the Government of India, in exercise of its powers under the Prevention of Cruelty to Animals Act, 1960, promulgated the Animal Birth Control Rules, 2001, subsequently amended and supplemented from time to time. These Rules established the **Capture-Sterilize-Vaccinate-Release (CSVR) model** as the principal method for controlling the stray dog population, thereby prohibiting indiscriminate culling of stray dogs and mandating municipal authorities to manage sterilisation, vaccination, and sheltering in coordination with animal welfare organisations. However, the implementation of these Rules has been ineffective, to say the least, across jurisdictions and the persistence of stray dog population has continued to imperil public safety in many parts of the country.

16. It has also been brought to the notice of this Court through a report published by NDTV[1], that even foreign nationals visiting India are falling prey to unprovoked stray dog attacks. In one such incident which took place in Bengaluru, a Welsh entrepreneur was bitten by a stray dog during a morning run. This incident underscores that the menace is neither confined to rural or densely populated localities nor limited to vulnerable citizens, but has assumed proportions that affect public safety, tourism, and the image of the country in the global perspective.

17. In addition, particular vulnerability has been observed in institutional spaces such as educational institutions, hospitals, sports complexes, bus stands/depots (including Inter-State Bus Terminals) and railway stations. These facilities/places, by virtue of their open design, congregation of persons and frequent availability of edible waste, provide favourable conditions for the habitation of free-roaming stray dogs. Reports from across India have

[1] **Welsh Entrepreneur Bitten by Stray Dog During Run in Bengaluru: 'Ask Dogesh Bhai...; LINK:** https://www.ndtv.com/offbeat/welsh-entrepreneur-bitten-by-stray-dog-during-run-in-bengaluru-ask-dogesh-bhai-9489758/amp/1.

demonstrated that such premises have repeatedly become scenes of dog-bite incidents, causing injuries to students, patients, staff and members of the public, thereby underscoring the urgent need for targeted preventive and administrative measures.

I. <u>Educational institutions (schools, colleges, universities, and coaching institutions with/without residential/hostel facilities)</u>

18. Educational institutions, particularly schools and colleges with open campuses, have emerged as areas of recurring dog-bite incidents. Children, due to their small stature and uninformed interaction with animals, are extra vulnerable to the same. Several reported incidents have emerged over the years, where students have sustained grievous injuries within school/college premises or adjacent playgrounds as a result of dog bites. Such cases have, in several instances, necessitated surgical reconstruction and emergency prophylactic treatment for rabies. The frequency of such incidents reflects deficiencies in institutional responsibility and municipal oversight concerning the safety of educational environments. We are informed that the

Campus of National Law School of India University, Bengaluru has a huge population of strays which threaten the safety of the students, staff and faculty members alike.

Incidents:

- At a **Government Lower Primary School, Panamaram, Wayanad, Kerala**, a Class III student was bitten by a stray dog inside a classroom. The dog had given birth to pups near a wash basin in an abandoned corner of the school building (which had not been locked after vacation).[2]
- In **Siswal village, Hisar district, Haryana**, a stray dog entered a government primary school, bit six students, then also bit others in the village.[3]
- Students from college within **Bengaluru University campus** were bitten by stray dogs while on campus (Kengeri area). Two college students were hospitalised after the attack.[4]

---

[2] **Stray dog bites student inside classroom in Wayanad school; LINK:** https://www.onmanorama.com/news/kerala/2025/09/08/stray-dog-bites-studnet-in-wayand-school.html.

[3] **Stray dog bites 6 students in Hisar Village school; LINK:** https://timesofindia.indiatimes.com/city/chandigarh/stray-dog-bites-6-students-in-hisar-village-school/articleshow/123953280.cms.

[4] **Karnataka records 2.86 lakh dog bites, 26 rabies deaths this year, report reveals; LINK:** https://www.indiatoday.in/india/karnataka/story/karnataka-dog-bites-deaths-2025-rabies-stray-dogs-supreme-court-order-delhi-ncr-data-2770508-2025-08-13.

II. Hospitals and healthcare institutions

19. Ironically, the very institutions entrusted with the treatment of dog-bite victims, have themselves become susceptible to the menace. In hospitals and several tertiary-care centres, patients, attendants and staff have been attacked by packs of dogs residing within hospital compounds. The problem is exacerbated by improper waste disposal practices and the presence of open areas that attract animals. In addition, the continuous inflow of dog-bite victims has strained medical resources, particularly the availability of anti-rabies vaccines and immunoglobulins, which are often in short supply.

Incidents:

- At **Institute of Mental Health (IMH), Kilpauk, Chennai**, multiple patients were bitten by stray dogs in a few days.[5]
- At **Ernakulam General Hospital, Kochi**, a stray dog attacked five people. Four of those were inside the hospital premises, including a patient.[6]

---

[5] **Stray dogs hound IMH patients, three bitten in three days; LINK:** https://timesofindia.indiatimes.com/city/chennai/stray-dogs-hound-imh-patients-three-bitten-in-three-days/articleshow/120561697.cms.

[6] **Stray dog attacks five on Ernakulam General Hospital premises; LINK:** https://www.newindianexpress.com/cities/kochi/2025/Aug/14/stray-dog-attacks-five-on-ernakulam-general-hospital-premises.

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)
Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

- The NHRC took *suo motu* notice of reports of dog-bite incidents involving patients within the hospital premise at **Acharya Harihar Post Graduate Institute of Cancer (AHPGIC), Cuttack, Odisha**. Some patients claimed that vital procedures (chemotherapy, radiation) were delayed because of such attacks.[7]
- At **Government Medical College and Hospital, Nagpur**, a resident doctor was bitten by several stray dogs in the hospital campus. She required ICU care. There have been multiple similar incidents over preceding days.[8]
- In **King George's Medical University (KGMU), Lucknow**, two doctors, paramedical staff and an attendant were bitten by a stray dog on campus, outside the radiology department.[9]

---

[7] **NHRC takes cognizance of TNIE report, issues summons to Odisha govt on stray dog menace in cancer hospital; LINK:** https://www.newindianexpress.com/states/odisha/2023/May/25/nhrc-takes-cognizance-of-tnie-report-issues-summons-to-odisha-govt-on-stray-dog-menace-in-cancer-ho-2578550.html.

[8] **Nagpur's premier medical facility battles dog menace; woman doctor in ICU after attack; LINK:** https://theprint.in/india/nagpurs-premier-medical-facility-battles-dog-menace-woman-doctor-in-icu-after-attack/1063457/.

[9] **In Lucknow, King George's Medical University doctors among 5 injured in dog attack; LINK:** https://timesofindia.indiatimes.com/city/lucknow/in-lucknow-king-georges-medical-university-doctors-among-5-injured-in-dog-attack/articleshow/100171596.cms.

III. Sports complexes and stadia

20. Large sports venues and open recreational grounds attract free-roaming/stray dogs because they offer food (from vendors and visitors) and hiding/denning space. As cities expand, many older municipal stadia and public playgrounds have become semi-permanent habitats for dog packs. During major events the concentration of people increases the chance of human-dog interactions and when a dog feels threatened or is provoked, injuries can follow.

Incidents:

- Two foreign coaches (from Kenya and Japan) were bitten by stray dogs inside **Jawaharlal Nehru Stadium, New Delhi, during the World Para Athletics Championships, 2025.** One coach was bitten near the competition arena and the other at the warm-up track. Both were treated at the stadium first, then at Safdarjung Hospital. These incidents show that even high-security venues can

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)
Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

be vulnerable if feeding and perimeter management are not enforced.[10]

IV. Bus stands/depots (including Inter-State Bus Terminals) and railway stations

21. This Court also takes cognizance of numerous reported incidents of stray dog attacks at public transport hubs, including bus stands/depots (particularly Inter-State Bus Terminals) and railway stations across several States. These facilities, by reason of heavy public congregation, open architecture, and unhygienic waste disposal practices, have become focal points for stray dog habitation, resulting in repeated assaults/attacks on commuters, employees, and bystanders.

Incidents:

- At **Kannur Railway Station, Kerala,** a stray dog reportedly bit 18 people at the station (on the platform and near the ticket counter) and the animal was later confirmed to have rabies. News article further indicated that residents and

[10] **Horrific! Stray dogs attack foreign coaches at World Para Athletics Championships, fifth such incident at JLN stadium; LINK:** https://timesofindia.indiatimes.com/sports/more-sports/athletics/horrific-stray-dogs-attack-foreign-coaches-at-world-para-athletics-championships-fifth-such-incident-at-jln-stadium/articleshow/124300397.cms.

commuters estimate the presence of over a hundred stray dogs in and around the station premises, resulting in a sustained risk to public health and passenger safety.[11]

- At **Dombivli Railway Station, Maharashtra,** a stray dog bit nine commuters, including a Railway Protection Force (RPF) Officer, on a foot over-bridge and platform.[12]
- At **Alappuzha Railway Station, Kerala,** more than 30 people were reported bitten by stray dogs in the past six months at the station premises.[13]
- At **Sambhal Railway Station, Uttar Pradesh,** a rabid/mad dog entered the railway station precinct and bit eight persons at different spots in about two hours.[14]

---

[11] **Rabies confirmed in dog that bit 18 people at Kannur railway station; LINK:** https://www.newindianexpress.com/states/kerala/2024/Nov/29/rabies-confirmed-in-dog-that-bit-18-people-at-kannur-railway-station.

[12] **Stray dog bites commuters at Dombivli railway station; LINK:** https://www.mid-day.com/mumbai/mumbai-news/article/stray-dog-bites-commuters-at-dombivli-railway-station-23596600.

[13] **Over 30 people bitten by dogs at Alappuzha Railway Station in 6 months; LINK:** https://english.mathrubhumi.com/news/kerala/over-30-people-bitten-by-dogs-at-alappuzha-railway-station-6-months-17c1a66c.

[14] **Rabid dog bites eight people at city railway station; LINK:** https://www.jagran.com/uttar-pradesh/sambhal-city-mad-dog-terrorizes-railway-station-injures-several-40014446.html.

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)
Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

- At **Kannur Bus Stand, Kerala,** a stray dog attacked about 50 people, including at the bus-stand premises.[15]
- At **KSRTC Bus Stand, Kottayam, Kerala,** several people (including a former municipal chairperson) were injured in a stray dog attack that started around the bus stand and footpath routes mid-afternoon.[16]

22. The Court notes that the underlying causes of this enduring menace are multifaceted, including, **(i)** uncontrolled reproduction of stray dogs owing to inadequate implementation of sterilisation programmes; **(ii)** improper disposal of food waste in and around public institutions; **(iii)** absence of effective perimeter management and institutional coordination with municipal authorities; and **(iv)** lack of widespread public awareness regarding preventive conduct and post dog-bite medical procedures.

23. Despite the statutory framework of the Animal Birth Control Rules, 2001 as amended in 2023, and

---

15 **Stray dog attacks 50 people in Kannur town; LINK:** https://timesofindia.indiatimes.com/city/kozhikode/stray-dog-attacks-50-people-in-kannur-town/articleshow/121916268.cms.

16 **Stray dog attacks panic Kottayam bus stand, several injured. LINK:** https://www.onmanorama.com/news/kerala/2025/08/21/stray-dog-attack-kottayam.html.

the existence of various municipal bye-laws/guidelines/Standard Operating Procedures, the practical outcomes have remained suboptimal. The data emerging from several States and Union Territories reveal a year-on-year increase in reported dog-bite cases, many occurring within or near public institutions. The persistence of the problem calls for a holistic and coordinated approach involving municipal corporations, public health authorities, and administration of the institutions, to ensure that the constitutional mandate of safeguarding the right to life under Article 21 is not compromised by administrative inaction or inefficiency.

24. The menace of dog bites, particularly in public and private institutions that serve as spaces of learning, healing and recreation, thus constitutes not merely a public-health challenge but a matter of human safety concern. The State and its instrumentalities bear an affirmative obligation to ensure that no citizen, least of all children, elderly people and patients, are exposed to preventable injury or disease within public premises.

IV. Directions

25. Having regard to the alarming rise in incidents of dog bites within institutional areas such as educational institutions, hospitals, sports complexes, bus stands/depots (including Inter-State Bus Terminals) and railway stations, this Court deems it appropriate to issue the following directions in the interest of public safety, health, and management of stray dogs: -

A. The State Governments and Union Territories shall through their respective local/ municipal authorities, within a period of two weeks, identify all Government and private educational institutions, hospitals (including district hospitals, primary health centres, and medical colleges), public sports complexes or stadia, bus stands/depots (including Inter-State Bus Terminals) and railway stations situated within their territorial limits.

B. The administrative heads of the aforesaid institutions shall through their respective local/ municipal authorities, under the overall supervision of the District Magistrate concerned,

ensure that the premises are secured by adequate fencing, boundary walls, gates and such other structural or administrative measures as may be necessary to prevent the ingress of stray dogs. The said exercise shall be completed as soon as possible and preferably within a period of 8 weeks from today.

C. The management of every educational institution, hospital, sports complex, bus stand/depot (including Inter-State Bus Terminal) and railway station identified under **Direction (A)** shall designate a Nodal Officer responsible for the upkeep and cleanliness of the premises and for ensuring that stray dogs do not enter or inhabit the campus. The details of the said officer shall be displayed prominently at the entrance and notified to the jurisdictional municipal body/authority.

D. The local municipal authorities and panchayats shall carry out regular inspections, at least once in every three months, of all such premises to ensure that no stray dog habitats exist within or in the immediate vicinity of these institutions. Any lapse in this regard shall be viewed seriously, and

responsibility shall be fixed upon the concerned municipal officials/administrative authorities.

E. It shall be the responsibility of the jurisdictional municipal body/authority to forthwith remove every stray dog found within the premises of an educational institution, hospital (public or private), sports complex, bus stand/depot (including Inter-State Bus Terminal) or railway station and to shift such animal/s to a designated shelter, after due sterilisation and vaccination, in accordance with the Animal Birth Control Rules, 2023. The stray dogs so picked up shall not be released back to the same location from which they were picked up. We have consciously directed the non-release of such stray dogs to the same location from which they were picked up, as permitting the same would frustrate the very effect of the directions issued to liberate such institutional areas from the presence of stray dogs.

F. All Government and private hospitals shall maintain a mandatory stock of anti-rabies vaccines and immunoglobulin at all times.

G. Every school and educational institution shall be directed by the Ministry of Education, Government

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)
Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

of India, to conduct awareness sessions for students and staff on preventive behaviour around animals, first-aid in case of bites, and immediate reporting protocols.

H. The management of stadiums and sports complexes shall ensure the deployment of security or ground-keeping personnel specifically tasked with around the clock vigil against the entry or habitation of stray dogs.

I. The railway authorities having jurisdiction over the railway stations as well as the State transport corporations and municipal authorities having jurisdiction over bus stands, depots and Inter-State Bus Terminals, shall ensure that such public-transport premises/facilities are effectively secured and maintained so as to prevent the habitation or movement of stray dogs within their premises. Proper waste-management systems shall be implemented to eliminate food sources that attract animals, and regular inspections shall be conducted to detect and address the presence of stray dogs.

J. Animal Welfare Board of India shall, within four weeks, issue detailed Standard Operating

Procedures (SOPs) for prevention of dog bites and management of stray dogs in institutional premises (public or private) including but not limited to Government and private educational institutions, hospitals (including district hospitals, primary health centres, and medical colleges), and sports complexes or stadia, to be uniformly adopted across all States and Union Territories.

26. The aforesaid directions are being issued in continuation of and in furtherance of this Court's order dated 22nd August, 2025, to ensure that the menace of stray dog attacks within institutional areas is curbed through effective preventive and administrative mechanisms. The primary objective is to safeguard the fundamental right to life and safety of citizens, particularly children, students, patients, and sportspersons, while ensuring compliance with the principles embodied in the Animal Birth Control Rules, 2023 framed under the Prevention of Cruelty to Animals Act, 1960.

27. The Registry shall forthwith circulate a copy of this order to the Chief Secretaries of all States and Union Territories for onward transmission to all the

necessary departments, as well as to the Secretaries of the Ministry of Health and Family Welfare; Ministry of Education; Ministry of Fisheries, Animal Husbandry and Dairying; Ministry of Youth Affairs and Sports; Ministry of Road Transport and Highways; Ministry of Railways; Ministry of Panchayati Raj; Ministry of Rural Development; and Chairman, National Highways Authority of India, for immediate compliance.

28. The Chief Secretaries of all States and Union Territories shall file their affidavits of compliance before this Court within a period of 8 weeks from today, specifically indicating:

i. the steps taken to secure the premises of the educational institutions, hospitals, sports complexes, bus stands/depots (including Inter-State Bus Terminals) and railway stations;

ii. the mechanism put in place for regular oversight inspection, coordination and reporting with municipal authorities/Panchayati Raj institutions; and

807

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)

Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

iii. the availability of anti-rabies vaccines and immunoglobulin in all Government medical facilities.

29. The Union of India shall also ensure that the aforesaid directions are implemented in respect of all institutional areas falling under its administrative or supervisory control, including Central Government educational institutions, hospitals, colleges, universities, sports complexes and railway stations managed by or affiliated with Central Ministries or authorities such as the Ministry of Health and Family Welfare; Ministry of Education; Ministry of Fisheries, Animal Husbandry and Dairying; Ministry of Youth Affairs and Sports; Ministry of Road Transport and Highways; Ministry of Railways; Ministry of Panchayati Raj; Ministry of Rural Development and other allied departments. The Union of India, through the Ministry of Health and Family Welfare, shall file a comprehensive affidavit of compliance within a period of 8 weeks from today, indicating the steps taken to secure such institutions, the mechanism evolved for coordination with local/municipal authorities, and the measures adopted for ensuring the availability of

808

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)
Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

anti-rabies vaccines and immunoglobulin in Central Government hospitals and healthcare facilities.

30. Animal Welfare Board of India shall also file a consolidated report indicating the nationwide status of sterilisation and vaccination drives, as well as the formulation of uniform Standard Operating Procedures for the prevention of dog-bite incidents in institutional areas/premises within 8 weeks from today.

31. The Registry shall forthwith implead the Urban Development Department and Rural Development Department of all States and Union Territories as well as the Union of India through their Principal/Chief Secretaries.

32. Any reported non-compliance of any of the above directions shall be viewed very seriously and may invite penalties/consequences including but not limited to the initiation of *suo moto* contempt proceedings against the erring officials.

33. The matters shall be listed on 13th January, 2026 for further directions and for perusal of the compliance affidavits to be filed by the Animal

Welfare Board of India, all the States and Union Territories and the Union of India.

.....J.
(VIKRAM NATH)

.....J.
(SANDEEP MEHTA)

.....J.
(N. V. ANJARIA)

NEW DELHI;
NOVEMBER 07, 2025.

File No. Z.28016/114/2025-PMSSY-I (Computer No. 8377953)
Generated from eOffice by VIJAY KUMAR GUPTA, US(VKG)-PMSSY-I-MOHFW, UNDER SECRETARY, DOHFW DEPARTMENT on 09/12/2025 06:04 pm

DEALED IN MY PRESENCE

Z.28016/114/2025-PMSSY-I (8377953)
भारत सरकार
स्वास्थ्य एवं परिवार कल्याण मंत्रालय
स्वास्थ्य एवं परिवार कल्याण विभाग
पीएमएसएसवाई-I

निर्माण भवन, नई दिल्ली
दिनांक: 09-12-2025

To

The Director/Executive Director,
All New AIIMS under PMSSY

Subject: Compliance with the direction of the Hon'ble Supreme Court in Suo Motu W.P. (C) No. 5/2025 titled "IN RE:CITY HOUNDED BY STRAYS, KIDS PAY PRICE"- reg

Sir/Ma'am

I am directed to forward Ministry of Health & Family Welfare OM No.Z.21020/242/2025-PH dated 03.12.2025 alongwith Hon'ble Supreme Court order in the above matter for necessary compliance.

2. The matter may be taken on **'Top Priority'** and the compliance report may be furnished to this Department by 15.12.2025 for further necessary action.

Digitally signed by
Vijay Kumar Gupta
Date: 09-12-2025
18:03:35
(विजय कुमार गुप्ता)
भारत सरकार के अवर सचिव
फ़ोन: 011-23061343

Copy to:-

i. The DDA, All AIIMS under PMSSY.
ii. All Deputy Secretary/Joint Directors (PMSSY Division)

Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Fwd: Advisory for timely processing of payment of GeM Bills -reg.

1 message

DDA AIIMS PATNA <dda@aiimspatna.org> Thu, Dec 18, 2025 at 11:13 AM
To: Shivanshu Shekhar <shivanshu12623@aiimspatna.org>

Regards,
Deputy Director (Admin.)
AIIMS, Patna
801507

---------- Forwarded message ---------
From: **Mr Sourabh** <pmssy5-mohfw@gov.in>
Date: Wed, Dec 17, 2025 at 10:48 AM
Subject: Advisory for timely processing of payment of GeM Bills -reg.
To: director <director@aiimsbhopal.edu.in>, director <director@aiimsbhubaneswar.edu.in>, director <director@aiimsjodhpur.edu.in>, director <director@aiimspatna.org>, director <director@aiimsraipur.edu.in>, director <director@aiimsrishikesh.edu.in>, edaiimsrbl <ed.aiimsrbl@gmail.com>, director <director@aiimsmangalagiri.edu.in>, directoraiimsnagpur <directoraiimsnagpur@gmail.com>, ed <ed@aiimskalyani.edu.in>, executivedirector <executivedirector@aiimsgorakhpur.edu.in>, director <director@aiimsbathinda.edu.in>, director <director@aiimsguwahati.ac.in>, executive-director <executive-director@aiimsguwahati.ac.in>, edaiimsbls <edaiimsbls@gmail.com>, director <director@aiimsbilaspur.edu.in>, director <director@aiimsdeoghar.edu.in>, rakeshkumar7123 <rakeshkumar7123@yahoo.in>, edaiimsrajkot <ed.aiimsrajkot@gmail.com>, directoraiimsbbnagar <director.aiimsbbnagar@gmail.com>, madhabananda <madhabananda@gmail.com>, drmhraosvims1957 <drmhraosvims1957@gmail.com>, shakti810505 <shakti810505@gmail.com>, director <director@aiimsjammu.edu.in>, sachimohanty <sachimohanty@rediffmail.in>
Cc: dydir <dydir@aiimsbhopal.edu.in>, dda <dda@aiimsbhubaneswar.edu.in>, dda <dda@aiimsjodhpur.edu.in>, dda <dda@aiimspatna.org>, dda <dda@aiimsraipur.edu.in>, dda <dda@aiimsrishikesh.edu.in>, ddaaiimsrbl <ddaaiimsrbl@gmail.com>, dda <dda@aiimsnagpur.edu.in>, kpradip10 <kpradip10@gmail.com>, dda <dda@aiimsgorakhpur.edu.in>, ashwanimahaur <ashwanimahaur@gmail.com>, rajeevsenroy30 <rajeevsenroy30@gmail.com>, ddaaiimsbilaspur <ddaaiimsbilaspur@gmail.com>, dda <dda@aiimsbilaspur.edu.in>, dda <dda@aiimsdeoghar.edu.in>, ddamadurai1189 <ddamadurai1189@gmail.com>, ddaaiimsrajkot <dda.aiimsrajkot@gmail.com>, ddaaiimsbibinagar <dda.aiimsbibinagar@gmail.com>, dda <dda@aiimsguwahati.ac.in>, ddaaiimsjammu <ddaaiimsjammu@gmail.com>, macprasad <mac.prasad@gmail.com>, ddaaiimsawantipora1 <ddaaiimsawantipora1@gmail.com>, dda <dda@aiimsmangalagiri.edu.in>, Aditya Kumar Mamgain <mamgain.aditya@lss.sansad.in>, Dharm SIngh <dharmbk.singh@nic.in>, Sourabh <sourabh.12@gov.in>, dhananjay90 <dhananjay.90@gov.in>

आदरणीय महोदय/महोदया,

उपर्युक्त विषय के संदर्भ में, कृपया संलग्न अनुलग्नक देखें।

सादर
पीएमएसएसवाई-V
निर्माण भवन

512-बी, ए विंग,
नई दिल्ली-110011

Ministries letter dated 16.12.2025.pdf
89K

File No. Z-28016/143/2025-PMSSY-V(8371177)
Government of India
Ministry of Health & Family Welfare
Department of Health & Family Welfare
(PMSSY-V Section)
****

Nirman Bhawan, New Delhi
Dated:16-12-2025

To

The Executive Director, all AIIMS under PMSSY

Subject: Advisory for timely processing of payment of GeM Bills -reg.

Sir/Madam,

I am directed to refer to the above-mentioned subject and to say that several complains/representations are being received in the Ministry from time to time regarding undue delays in the processing and clearance of their GeM bills by few AIIMS.

2. As you are aware that the Government of India's guidelines on GeM procurement, and the General Financial Rules (GFR) mandate that payments must be released within the stipulated period to ensure transparency, credibility and smooth functioning of procurement processes.

3. Accordingly, all Executive Directors of AIIMS under PMSSY are advised to review their respective pendency of GeM bills on a monthly basis and ensure that GeM bills are processed for payment within the prescribed timelines as per rules in place on the subject

4. This issues with the approval of Competent Authority.

Yours faithfully,

Digitally signed by
Dharm Bir Kumar Singh
Date: 16-12-2025
13:04:36

(Dharm Bir Kumar Singh)
Under Secretary to the Govt. of India
Tel: 011-23062319

Copy to:

DDA, all AIIMS under PMSSY.