ANDHRA PRADESH TECHNOLOGY SERVICES LIMITED
(Government of AP Undertaking)
(CERT-In Empanelled and ISO 9001:2015, ISO 27001:2013 Certified)
3rd Floor, R&B Building, Opp. Indira Gandhi Municipal Stadium,
MG Road, Labbipet, Vijayawada-520010, Andhra Pradesh, India.
Ph.0866-2468108 | md_apts@ap.gov.in |https://www.apts.gov.in/

02 25/7/25

Lr.No ITC51-20023/14/2019-IS AUDIT-APTS, Dated: .07.2025

Respected Sir/Madam,

Sub: APTS - Cyber Security – Protection of Government's ICT infrastructure, Digital Assets from Cyber-attacks - Communication of Security Guidelines, SOP to enhance the Cyber Security Posture of Critical Sector Entities - Reg.

Ref:
1. Director General, Ministry of Electronics and Information Technology (MeitY), Govt of India, NIC, DO.No. 3(1)/2025/2, dated:10.05.2025.
2. National Security Council Secretariat, Cyber Wing, NSCS ID No 46/87/2025-NSCS (CS), dated:07.05.2025.
3. Home Secretary, Government of India, New Delhi D.O.No.22014/12/2025-CS, dated:07.05.2025.
4. National Cyber Security Policy - 2013" on 02.07.2013
5. G.O.Ms.No.2, dated 01.03.2017- Andhra Pradesh Cyber Security Policy
6. G.O.Ms.No.4 dated 10.01.2019 issued by ITE&C dept., GoAP

---o0o---

Kind attention requested on the above subject and references cited.

Vide ref (1) cited, the Director General, MeitY, Govt. of India, has highlighted the increasing risk of cyber-attacks targeting Government ICT infrastructure and applications. It is emphasized that all the digital assets under Government Departments must be closely monitored & protected.

Further, a copy of the comprehensive guidelines issued by the National Informatics Centre (NIC) covering the following aspects are forwarded with a request to ensure strict adherence to the guidelines (enclosed as Annexure-I):

1. End-point security
2. Application security
3. Infrastructure security
4. Network security
5. Email security
6. Business continuity and cyber crisis management
7. Cyber security awareness

To for
n/e
A. Mani
29/7/25

Vide ref (2) cited, National Security Council Secretariat, Cyber Wing has informed that, 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 the stakeholders. A Standard Operating Procedure (SOP) has been issued to enhance the cybersecurity posture of critical sector entities (enclosed as Annexure-II) and requested that all the stakeholders implement the provisions of the SOP in their respective sectors and work proactively to ensure the Cybersecurity postures of their respective entities.

Vide ref (3) cited, the Home Secretary, Government of India, New Delhi has informed that, Cyber Multi Agency Centre (CyMAC) has been established at New Delhi under the

Ministry of Home Affairs to effectively address cyber espionage, cyber terrorism, cybersecurity threats/incidents, misuse of emerging technologies against national security & similar concerns and requested that all the Cyber attacks / incidents / events such as Defacement, Distributed Denial of Service (DDoS) attacks, Phishing campaigns, etc., may be immediately reported to following CyMAC Control Room Numbers:

i. Landline: 011-23094060
ii. Mobile: +91-9599660733
iii. Email: cycordadmin.mha@gov.in
iv. MAC IP Phone: 779903-05 (Only for MAC Network connected agencies)

Further, it is to inform that, GoI issued National Cyber Security Policy - 2013" on 02.07.2013. To complement and supplement "National Cyber Security Policy 2013", Government of Andhra Pradesh (GoAP), vide ref (5) cited, issued "Andhra Pradesh Cyber Security Policy (APCSP)" with a vision "to create a robust ecosystem, wherein the citizens can transact online securely and take steps to protect their identity, privacy and finances online, the businesses conduct their operations without any disruption or damage and the Government ensures that its data and ICT systems are secure".

Vide ref (6) cited, the ITE&C Department identified M/s APTS Ltd, as a Nodal agency for implementing APCSP. Accordingly, APTS established the AP Cyber Security Operations Centre (APCSOC) in Vijayawada on 23.04.2018 to monitor (24/7) all the critical IT Infrastructure of GoAP onboarded to APCSOC.

Further, it is to inform that, APTS was empanelled with CERT-In, GoI for providing the Cyber Security Audit & Assurance Services. The contact details for utilizing these services are:

i. Landline: 0866-2468123,
ii. Mobile: +91-9440469194
iii. eMail: mgr-apcsp-apts@ap.gov.in

In view of the above, you are requested to kindly make necessary arrangements to ensure strict adherence to the prescribed Cybersecurity protocols. This matter may please be treated as very important, as it is essential for safeguarding sensitive Government digital infrastructure and preventing potential cyber-attacks.

Yours faithfully,

Digitally signed by
SURYATEJA MALLAVARAPU
Date: 04-07-2025
11:41:09

Managing Director

To,
All AP Secretariat Departments,
All District Collectors, AP
All Head of Departments of GoAP
All Heads of AOs of GoAP

अभिषेक सिंह, भा.प्र.से.
महानिदेशक

Abhishek Singh, IAS
Director General

सत्यमेव जयते

भारत सरकार
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
राष्ट्रीय सूचना–विज्ञान केन्द्र

Government of India
Ministry of Electronics and Information Technology
National Informatics Centre

Spl-Secretary

URGENT/IMMEDIATE

DO No:3(1)/2025/2
Date: 10-5-2025

Dear Sir / Madam,

With the recent developments, it has been observed that possibilities of cyber-attacks on ICT infrastructure and applications has gone up. It is very essential keep close watch and continuous monitoring of all out digital assets. It is advisable to strictly adhere to security guidelines issues by various agencies from time to time and to adopt the best practices to protect Government's ICT infrastructure from becoming prey to these attacks.

All concerned must ensure that the digital assets under your jurisdiction are protected and checked on daily basis and the status of digital assets and infrastructure is reported.

Guidelines and framework for end-point security, application security, infrastructure security, network security, email security, business continuity and cyber crisis management and cyber awareness are enclosed for your immediate reference.

You may please circulate to the all concerned officials in the Ministry/Department and Organizations attached to the Ministry/Departments to strict adherence to the guidelines. For any support from NIC, our teams can be reached out anytime as our control room is functional round the clock (Phone: 011-24305116/22902414), email: incident@nic-cert.nic.in)

With regards

Yours Sincerely

10/05/25
(Abhishek Singh)

To:

1. All CISOs/Deputy CISO (Ministries/Departments)
2. All HOGs & HODs (NIC Ministries/Departments)
3. SIOs NIC States/UTs

CC:

1. All Secretaries to Govt. of India
2. All Chief Secretaries of States/UTs
3. JS, Cabinet Secretariat,
4. JS, PMO, New Delhi
5. NSCS, New Delhi
6. Director General, CERT-In

Encl. as above:

1. Endpoint Security (Annexure-1)
2. Application Security (Annexure-2)
3. Network Security (Aneexure-3)
4. Email Security (Annexure-4)
5. Business continuity and cyber crisis management (Annexure-5)
6. Cyber Security Awareness (Annexure-6)
7. Template for reporting Cybersecurity of Digital assets

Template for reporting Cybersecurity of Digital assets

Date: ___/___/ 2025

Name of the Dept: ____

Ministry: ____

Details of Digital Assets:

1. Number of Applications :

   (Please provide details for each of the application as separate annexure)

   Name of the application **Status: Up/Down Remarks:**
2. Hosting Data Centre :
3. Number of Critical applications :
4. Number of users typically access the porta/applications
5. Number application URLs other than "gov.in/nic.in":
6. Number of applications on CDN :
7. (list of applications may be enclosed as separate annexure)
8. Number of applications behind WAF :
9. Number applications geofenced (only access with in Indian territory)

Incidents and Status:

1. Incidents happened to the applications

   (please provide details applications wise including Date of the incident, date of reporting and rectification/mitigation activity carried out, if any)
2. DDOS attacks
   a. Intensity of attack
   b. Duration of attack
3. Attempted Intrusions
   a. Blocked intrusions
   b. Affected by intrusion
   c. Type of disturbance
4. Attempted access by bad reputed IPs

5. Any other information relevant to perfornace:

Annexure-1

Endpoint Security

1. Only endpoints with licensed Operation system (i.e., desktops, laptops, workstations) to be connected to the network.
2. All desktops shall be installed with Endpoint security solution such as Antivirus/EDR, UEM before connecting to NIC network.
3. All desktops / laptops USB ports shall be disabled. Only enabled after due approval of CISO
4. All network devices shall have MAC-binding done on network switches
5. Host Firewall to be enabled on all endpoints, restricting lateral movement within the same network segment.
6. Administrator privileges to be revoked for all the endpoints.
7. All endpoints connecting to the NIC network to be configured with a common NIC DNS and NTP server.
8. Every endpoint should have logging enabled and logs should be reviewed regularly.
9. Only approved softwares to be installed on systems.
10. Access to systems, servers, devices, including printers, scanners etc. to be protected with a password.
11. Sensitive files to be stored in encrypted form or password protected.
12. Use of Remote access tools to be prohibited within organization network.
13. All operating systems to be kept up to date with the latest security patches.
14. Mobile Device Management
    - i. Mobile devices with sensory functions to be restricted within specified controlled zones where classified data is held.
    - ii. Mobile phone features such as Wi-Fi, GPS, Bluetooth and NFC should be kept disabled by default and only activated when necessary or grant permission to Apps only if necessary.

Advisory and Resource Facilitation
National Informatics Centre.
A-Block, CGO Complex, Lodhi Road,
New Delhi - 110003 India
IP No 5578
Csg-advisory@nic.in

NIC-CSG/2025-SPI/02
Dated: 10-05-2025

Annexure 2

Application Security

1. Ensure that the all applications/websites/services are hosted only at the designated data centers.
2. Critical Host applications after Comprehensively Security Audit by CERT-In empaneled agency.
3. Web software applications should be developed in accordance with secure coding guidelines such as the OWASP guidelines
4. WAF should be deployed to protect public-facing applications from threats such as SQL injection and cross-site scripting (XSS).
5. Use latest version of Web server, Database Server etc. Apply appropriate updates/patches on the OS and Application software expeditiously.
6. Unused services should be disabled in all applications and systems through proper security configurations.
7. Application security testing and vulnerability assessment should be performed at pre-defined frequency.
8. Periodically check the web server directories for any malicious/unknown web shell files and remove them as and when noticed.
9. All critical applications shall be placed behind WAF and shall be moved to safe hosting environment/secure data centers.
10. All servers shall be configured with Trusted NTP (samay1.nic.in) and DNS servers (1.10.10.10)
11. Access to Administrators and developers shall be through access rights management.
12. Access to the administrator, developers shall be through trusted connections such as ZTA, VPN.
13. Application logs to be monitored for unauthorized access attempts.
14. All the critical websites/applications to be continuously monitored by SOC and NOC.
15. All logs shall be corelated with threat feeds in real-time. Any abnormalities shall be escalated and mitigated immediately.
16. Use strong passwords, biometrics, MFA etc for providing secure access to the application user and administrators.
17. Administrative rights for system access should only be used only when required.
18. Inform immediately CERT-In and NCIIPC in case of any untoward incident.

Annexure 3

Network Security

1. Implement Network segmentation to enhance security and efficient network management.
2. Disable unused physical ports on network devices such as switches, routers, and wireless access points.
3. Use Firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) to monitor and block unauthorized access.
4. Monitor and replace end-of-life network components to prevent potential security vulnerabilities.
5. Continuously monitor traffic within and between segments. Analyse logs to detect anomalies that could indicate a security breach.
6. Use Air-gapped network for handling SECRET classified information
7. Implement role-based access with proper authentication and authorization to all network devices.
8. Do not user any other WiFi connections/broadband connections in the office.
9. Use secure communication using VPNs or Zero Trust Architecture (ZTA) for secure transmission of data while using public network.
10. Conduct regular vulnerability scans and penetration tests to Identify vulnerabilities.

Annexure 4

Email Security

1. Use strong password as per policy for accessing the email.
2. Do not reuse government email password elsewhere.
3. Access email from limited and sanitized devices.
4. Disable the "Save Password" feature in browsers.
5. Do not use government email id to register on social media, e-commerce platforms etc. and for non-official communications.
6. Do not click suspicious links and attachments in emails/SMS from unknown sources without verifying from official channels.
7. Do not respond to any unknown emails.
8. Do not forward or reply all unless required. Forward / reply with trail mail ONLY, if required.

Some ways to recognize a phishing email:

1. If a mail received from unknown source, this may be a source of phishing.
2. Be suspicious of emails that claim you must click, call, or open an attachment immediately or urgently.
3. If an email message has obvious spelling or grammatical errors, it might be a scam. e.g., nlc.in where the first "i" has been replaced by "l", or gov.in, where the "o" has been replaced by a "0" (zero).
4. Images of text used in place of text (in messages or on linked web pages) may be scam.
5. Be cautious of links containing short URL such as Bit.ly etc.

Annexure-6

Business continuity and cyber crisis management

1. Organization should maintain replica of its information at the Disaster Recovery (DR) site.
2. Copy of the database, configuration, golden image of critical server etc., should be stored offline.
3. Conduct DR, backup and restoration drills to ensure preparedness.
4. Ensure that the DR and BCP implementation is in line with the defined policies.
5. Establish a business continuity plan and conduct Business Impact Analysisat regular intervals.
6. Incorporate redundancy and failover strategies to prevent single points of failure.
7. Every organization should have Cyber Crisis Management Plan (CCMP) in place.

Annexure-5

Cyber Security Awareness

1. Social media

(a) Do not access social media from official devices, including personal devices with access to official information.

(b) Only designated officials should be allowed to access official social media handles from authorised systems.

(c) Duly approved content to be posted on official social media handles.

(d) No official information should be disclosed on personal social media handles.

2. Information Security Awareness and Training

(a) Regular training sessions to be conducted for officials to make them aware of evolving cyber security threat.

(b) Simulated exercises, such as phishing tests, to be conducted to assess the practical application of security protocols.

3. Reporting of Security Events

Cyber Incidents should be reported to CERT-In (incident@cert-in.org.in) or NCIIPC, as the case maybe, within 6 hours. Please refer the websites of CERT-In and NCIIPC for further details.

NATIONAL SECURITY COUNCIL SECRETARIAT
CYBER WING

1863/CSP/2025

Room No-205,
2nd Floor, Sardar Patel Bhawan,
Sansad Marg, New Delhi-110001

Spl. Secretary

SOP FOR CRITICAL SECTOR ENTITIES

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. A SOP has been created to enhance the cybersecurity posture of critical sector entities. The same is attached herewith as **Appendix**.

Secy ITE&C

2. It is requested that all stakeholders implement the provisions of the SOP in their respective sectors and work proactively to ensure the cybersecurity postures of their respective entities.

(Lt Gen MU Nair (Retd))
NCSC & Member Secretary, NCSA
Tele: 23451306

Chief Secretary, Government of Uttar Pradesh, Room No.101, 1st Floor, B Block, Lok Bhawan, Uttar Pradesh, Lucknow-226001

Chief Secretary, Andaman & Nicobar Administration Secretariat, Port Blair-744101

Chief Secretary, 1st Block, 1st Floor, Room No 214, Andhra Pradesh Secretariat, Velagapudi, Amravati-522503

Chief Secretary, Government of Arunachal Pradesh, 5th Floor, Block- II, Civil Secretariat, Itanagar-791111

Chief Secretary, Government of Assam, C Block, 3rd Floor, Assam Secretariat, Dispur, Guwahati-781006

Chief Secretary, Government of Bihar, Main Secretariat, Patna-800015

Chief Secretary, 4th Floor, Haryana Civil Secretariat, Sector 1, Chandigarh – 160019

Chief Secretary-IT, M-5-11, Mahanadi Bhawan, Mantralaya, Atal Nagar, Naya Raipur, Chhattisgarh-492002

Chief Secretary, Government of Dadra & Nagar Haveli and Daman & Diu, 1st Floor, Office of Secretary Public Works Department, Vidyut Bhawan, Kachigam, Nani Daman, Daman-396215

Chief Secretary, Govt of NCT of Delhi, Delhi Secretariat, IP Estate, New Delhi-110002

Chief Secretary, Government of Gujarat, 1 Block, 5th Floor, Gandhinagar-382010

Chief Secretary, Government of Goa, 203, 3rd Floor, Secretariat, Porvorim, Bardez, Goa-403501

Chief Secretary, Government of Himachal Pradesh, HP Secretariat, Shimla-171002

Chief Secretary, Jammu and Kashmir, Room No 2/7, 2nd Floor, Main Building Civil Secretariat, Jammu-180001

Chief Secretary, 1st Floor, Project Building, Dhurwa, Ranchi, Jharkhand-834004

Chief Secretary, Government of Karnataka, Room No.320,3rd Floor, Vidhana Soudha, Bengaluru– 560001

Chief Secretary, Government of Kerala, Secretariat, Thiruvanthapuram, Kerala-695001

Chief Secretary, Government of Madhya Pradesh, MP Mantralya, Vallabh Bhawan Bhopal (MP)-462004

Chief Secretary, Govt of Maharashtra, CS Office, Main Building, Mantralaya, 6th Floor, Madame Cama Road, Mumbai-400032

Chief Secretary, Government of Manipur, Manipur Secretariat, South Block, Imphal - 795001

Chief Secretary, Government of Meghalaya, Main Secretariat Building, Rilang Building Room No. 321, Meghalaya Secretariat Shillong-793001

Chief Secretary, Government of Mizoram, New Secretariat Complex, Aizwal - 796001

Chief Secretary, Government of Nagaland, Nagaland Civil Secretariat, New Secretariat Road, Kohima, Nagaland-797004

Chief Secretary, Government of Odisha, General Administration, Department of Odisha Secretariat, Bhubaneswar – 751001

Chief Secretary, Goubert Avenue, Puducherry-605001

Chief Secretary, Government of Punjab, Punjab Secretariat, Chandigarh-160017

Chief Secretary, Government of Rajasthan Secretariat, Jaipur, Rajasthan – 302005

Chief Secretary, Government of Sikkim, New Secretariat, Gangtok, Sikkim-737101

Chief Secretary, Government of Tamil Nadu, Secretariat, Chennai-600009

Chief Secretary, Government of Telangana, Block C, 3rd Floor, Telangana Secretariat, Khairtabad, Hyderabad

Chief Secretary, New Secretariat Building, PO: Secretariat, Agartala, Tripura-799010

Chief Secretary, Government of Uttarakhand, 4 Subhash Road, Uttarakhand Secretariat, Dehradun-248001

Chief Secretary, Govt of West Bengal, Nabanna 13th Floor, 325, Sarat Chatterjee Road, Mandirtala Shibpur, Howrah – 711102

Principal Secretary, Civil Secretariat, Leh, Ladakh- 194101

Shri Praful Patel, Hon'ble Administrator, Office of Lakshadweep Administrator, Secretariat building, Kavaratti Lakshadweep

Director, All India Institute of Medical Sciences (AIIMS), Ansari Nagar, New Delhi-110029

Chairman, AICTE, Nelson Mandela Marg, Vasant Kunj, New Delhi- 110070

Chairman, University Grant Commission, Bahadur Shah Zafar Marg, New Delhi-110002

Commissioner of Police, 17th Floor, Delhi Police Headquarters, Jai Singh Road New Delhi-110001

Chief Manager & Secretary, NABARD, 8th Floor 'B' Wing C-24, 'G' Block Bandra Kurla Complex East Mumbai

CMD, SIDBI, SIDBI Tower, 15 Ashok Marg Lucknow – 226001 (UP)

CMD, National Stock Exchange (NSE), NSE-Corporate Office, National Stock Exchange of India Ltd. Exchange Plaza, C-1, Block-G, Bandra Kurla Complex, Bandra (E), Mumbai-400051

CMD, Bombay Stock Exchange, BSE Limited, 25th Floor, BSE Building, PJ Towers, Dalal Street, Mumbai-400001

Lt Col Abhishek Verma, GM (IT) & Chief Information Security Officer (CISO), National Highway Authority of India (NHAI), G 5&6, Sector-10, Dwarka, New Delhi-110075

Secretary, Ministry of Commerce & Industries (MoCI), Room No 426, Vanijya Bhawan, New Delhi

Chief General Manager (BIS) and CISO, GAIL (INDIA) Limited GAIL Jublee Tower, B-35 & 36, Sector- 1, Noida- 201301

Deputy Director General, Confederation of Indian Industries, The Mantosh Sondhi Centre, 23, Intuitional Area, Lodhi Road, New Delhi -110003

NSCS ID No 46/87/2025-NSCS(CS) 07 May 2025

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.

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.

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.

C.R. FAX OUT NO: 113

E-10478062/CSP/2025

गोविंद मोहन, भा.प्र.से.
GOVIND MOHAN, IAS

CONFIDENTIAL

सत्यमेव जयते

गृह सचिव
Home Secretary
भारत सरकार
Government of India
नॉर्थ ब्लॉक / North Block
नई दिल्ली / New Delhi

D.O. No. 22014/12/2025-CS

Spl-Secretary

7th May, 2025

8प

Dear Chief Secretary,

CyMAC (Cyber Multi Agency Centre) has been established under Ministry of Home Affairs to effectively address cyber espionage, cyber terrorism, cybersecurity threats/incidents, misuse of emerging technologies against national security and similar concerns.

DGP
Secy ITE&C
pl forward

2. In view of the heightened cyber threats in the backdrop of current national security scenario, a 24x7 Cyber Multi Agency Centre (CyMAC) Control Room has been operationalised at New Delhi to effectively counter and respond to all kind of Cyber threats. The CyMAC Control Room, comprising of all relevant stake holders - including MHA, CERT-In, NCIIPC, DoT, NIC, I4C, etc. - would act as nodal point for coordinating and sharing of communication between different Cyber Security Agencies in India regarding cyber incidents/attacks and consequently implementing an effective response mechanism for countering, mitigation and recovery.

9/5

3. Apropos, it is requested that all Cyber attacks / incidents/events such as Defacement, Distributed Denial of Service (DDoS) attacks, Phishing campaigns, etc., may be immediately reported to the following CyMAC Control Room Numbers:

i.	Landline: 011- 23094060
ii.	Mobile: +91- 9599660733
iii.	Email: cycordadmin.mha@gov.in
iv.	MAC IP Phone: 779903-05 (Only for MAC Network connected agencies)

With regards,

Yours sincerely,

(Govind Mohan)

To

The Chief Secretaries of all States/UTs.