Ministry of Electronics & IT

National Consultative Workshop on "Strengthening Cyber Security Frameworks for State Data"

Posted On: 16 MAY 2026 8:10PM by PIB Delhi

The Ministry of Electronics and Information Technology (MeitY) convened the National Consultative Workshop on "Strengthening Cyber Security Frameworks for State Data" at The Ashok Hotel, New Delhi on 11 May 2026. The Workshop was chaired by Shri S. Krishnan, IAS, Secretary, MeitY, and was attended by Principal Secretaries, Secretaries and senior officers from State and Union Territory Governments, along with representatives from the Indian Computer Emergency Response Team (CERT-In), the National Informatics Centre (NIC), and senior officials of MeitY and NeGD.

The workshop constituted stage II of a four-stage departmental summit on “Strengthening Cyber Security Frameworks for State Data,” initiated by MeitY pursuant to Prime Minister Narendra Modi’s directions at the 5th National Conference of Chief Secretaries. The Workshop, conducted in partnership with NeGD, aims to produce a comprehensive national cybersecurity policy framework for State governments through structured consultations with all 36 States and Union Territories of India.

Addressing the Workshop, Secretary MeitY Shri S. Krishnan underscored the imperative of building a resilient and secure digital governance ecosystem through sustained, coordinated effort between the Government of India and State governments. He emphasised that the protection of citizen data, such as health records, land titles, educational credentials, and welfare databases, held in trust by State governments through the digitisation of public services, is a fundamental governance responsibility, not an administrative formality. With the Digital Personal Data Protection Act, 2023, becoming fully enforceable from 13 May 2027, he noted that cybersecurity preparedness is no longer a best-effort commitment but a legal obligation for every State department that holds citizen data. Genuine cybersecurity resilience, he stressed, rests on institutional commitment and not on technological investment alone.

Shri S. Krishnan, IAS, Secretary, Ministry of Electronics and Information Technology said "India's digital governance ecosystem must be not only expansive but resilient. The protection of citizen data held in trust by State governments is a governance responsibility and not merely a technical obligation. Every State must put in place the institutional architecture to discharge this responsibility: a notified policy, an empowered CISO, an operational Security Operations Centre, and a Crisis Management Plan that reaches every department. Cybersecurity is not an IT function. It is a governance imperative."

Secretary Krishnan outlined four foundational requirements for every State and Union Territory: (i) a formally notified Cyber Security Policy, periodically reviewed in alignment with national guidelines; (ii) an appointed and empowered Chief Information Security Officer (CISO) at the State level, with mandate and accountability cascaded to departments; (iii) an operational State Security Operations Centre (SOC), integrated with the Government SOC at NIC; and (iv) a Cyber Crisis Management Plan (CCMP) deployed, tested and known across all departments.

He drew attention to the need for regular review of Disaster Recovery systems and endpoint security, stressing that operational vigilance must be continuous rather than periodic. He reiterated the principle of Secure by Design, that cybersecurity must be embedded from the earliest stages of application development and procurement, not retrofitted after deployment.

Secretary Krishnan highlighted the growing and evolving threat posed by AI-enabled cyber attacks and called for proactive, forward-looking risk management frameworks in State IT systems. He underlined that the human and behavioural dimensions of cybersecurity are as consequential as any technical control. The awareness, discipline and cyber hygiene of government officials who operate public systems are critical determinants of security outcomes, and must be addressed through sustained capacity building, not technology deployment alone.

On building India's cybersecurity human capital, he highlighted the role of structured training and certification programmes for State officials, delivered through platforms including NeGD, the ISEA Project and iGOTKarmayogi, alongside regular cyber drill exercises to test and strengthen incident response readiness. Secretary Krishnan reiterated the Government of India's direction to prefer indigenously developed cybersecurity solutions meeting prescribed technical standards, in alignment with the Aatmanirbhar Bharat Abhiyan.

The workshop deliberated upon six national thematic areas identified through the consultative process:

i. Risk-based assessments and continuous security monitoring of State IT assets
ii. Securing State Data Centres (SDCs) and State Wide Area Networks (SWAN) with modern perimeter, endpoint and cloud security controls
iii. Strengthening incident detection, response and recovery through dedicated SOCs and State Computer Security Incident Response Teams (CSIRTs), under the technical umbrella of CERT-In
iv. Legacy application modernisation, Secure-by-Design principles and Zero Trust Architecture
v. Data classification, compliance with the Digital Personal Data Protection (DPDP) Act, 2023, and alignment with MHA’s National Information Security Policy and Guidelines (NISPG)
vi. Appointment of CISOs across State departments, capacity building, skilling and citizen cyber awareness programmes

Shri K. K. Singh, Joint Secretary, Cyber Security, MeitY, briefed participants on the four-stage Departmental Summit framework and the national cybersecurity policy architecture, and presented the initiative's overall mandate and objectives.

Dr. Sanjay Bahl, Director General, CERT-In, presented an overview of the national cybersecurity threat landscape, including sustained ransomware campaigns targeting government data repositories, AI-enabled phishing attacks, supply-chain compromises and risks arising from misconfigured cloud environments. He reaffirmed CERT-In’s commitment to extending technical support, threat intelligence and incident response assistance to State governments and called for every State to establish a formal State CSIRT under CERT-In’s technical umbrella.

Shri V. T. V. Ramana, Head of Group, Cybersecurity, NIC, outlined the security architecture of NIC-managed State systems, including the Government Security Operations Centre (GSOC), VAPT programmes and Zero Trust integration and underscored NIC’s ongoing commitment to being a continuous security partner to State governments.

Ms. Savita Utreja, Group Coordinator, Cyber Security, MeitY, anchored the policy framework briefing in Session II, presenting the evidence base for the six national themes and the regulatory framework governing State cybersecurity obligations, including those arising from the DPDP Act, 2023 and NISPG.

The Workshop also provided a dedicated platform for all participating States and Union Territories to present their current cybersecurity status, operational challenges and priority action areas across the six national themes. These presentations gave the Ministry a direct, granular account of ground-level implementation realities and inputs that will directly shape the national policy framework to be finalised at the August Summit.

Next Steps: State-Level Workshopsand National Summit

Following the National Consultative Workshop, all States and Union Territories will conduct internal State-Level Workshops (Stage III) which is to be completed by June 30, 2026. Thereafter, as an outcome of State-level internal workshops, structured State inputs are to be submitted to MeitY within a stipulated timeline. Based on inputs received from all States/UTs,the comprehensive Final Note on “Strengthening Cyber Security Frameworks for State Data”shall be prepared. The comprehensive final note, including key action points and priority reform areas, will be deliberated in the National Departmental Summit (Stage IV), scheduled for August 2026. A report of the National Departmental Summit (Stage IV), including the key action points and priority reform areas agreed upon by States and Union Territories, will be submitted to the Cabinet Secretariat.

****

MSZ