प्रशासनिक सुधार और लोक शिकायत विभाग
DEPARTMENT OF ADMINISTRATIVE REFORMS AND PUBLIC GRIEVANCES

WORKSHOP ON CYBER SECURITY

PANEL DISCUSSIONS

- **CURRENT CYBER SECURITY LANDSCAPE IN INDIA**

- **CYBER SECURITY CONSIDERATIONS BY DIFFERENT GOVERNMENT APPLICATION**

Address of V.Srinivas, IAS Secretary DARPG, & DPPW , DG NCGG at the Workshop on Cyber Security dated 7.10.2024

The Hon'ble Prime Minister in his interaction with Secretaries to Government of India on June 29, 2024 said

"Ministries/ Departments to take steps to make their IT systems adequately resilient and to sensitize their officers to ensure scrupulous adherence to cyber security guidelines and protocols. This should be a continuing endeavour."

Accordingly Ministry of Electronics and Information Technology has addressed all Ministries/ Departments to take necessary sensitization initiatives in consultation with CERT-IN which is the first responder to cyber-attacks.

Cyber Security was a plenary session theme in the 27th National e-Governance Conference at Mumbai. It was a substantive discussion which featured in the Mumbai Declaration and the follow-up action was decided after consultations with Director General CERT-IN that a workshop for all Ministries/ Departments of Government of India shall be convened on the subject with specific focus to platforms operated by DARPG and DPPW.

It is in this backdrop that DARPG has convened this workshop on Cyber Security, to discuss issues of cyber security in general and the cyber security issues regarding the digital platforms administered by DARPG and DPPW in particular namely e-Office, Bhavishya and CPGRAMS. This workshop would be part of the Special Campaign 4.0 initiatives for Cyber Swachhata Awareness. I am delighted that nearly 200 officials of Ministries/ Departments could attend today's workshop.

The first step is to visit the Cyber Swachhata Kenra at www.csk.gov.in to get the latest information on malware, security best practices, countermeasures, security tools and download the 'Free Bot Removal Tool" to secure/ disinfect their systems. The Cyber Swachhata Kendra's mandate is to create a secure cyber space by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections. The National Cyber Security Policy envisages creating a secure cyber eco system in the country.

The widespread adoption of digital platforms such as e-Office, Bhavishya, and CPGRAMS has significantly improved the accessibility and efficiency of government services for millions of citizens. In the years 2014-2024, Governance models have transformed from physical to digital. It is important that our digital assets are adequately protected by adopting best practices in cyber security. Secure cyber application design, development, implementation and operations are the mandate of system designers. Relying solely on post-development audits for security is inadequate. The Application Programming Interfaces where data connections connecting data to be shared with other applications have increased exponentially and have been identified as amongst the most frequently breached web applications. We need to adopt the best practices in API security that have been laid down by CERT-IN.

National e-Services Delivery Assessment (NeSDA) 2023: The Department, under its biennial evaluation of the progress of e-Services - NeSDA, evaluates the public service delivery of states/UTs and central Ministries on various parameters. ***'Information security and privacy'*** has been included as one of key assessment parameters.

Datasets in NeSDA 2023 indicate that

- The parameter improved in 2023 for 24 State/ UT portals compared to 2021, 21 State/ UT portals achieved a 100 percent score for this parament. Across all States/ UT portals the maximum increase of 49 percent was observed in UT portals.

- States/ UT's have ensured clear indication of online security measures on their portals such as https protocol, lock symbol on browser and symbols for 3rd party security alliances.

- All State/ UT portals have updated copyright statements on the portals and also have a disclaimer and privacy policy for user data collected online.

- Alerts by SMS and email inform users on the unauthorized access attempts on their profiles, password changes and other security related events.

- There are features for password recovery and reset features available as also automatic email notifications on password expiry.

This workshop on Cyber Security aims to equip Government of India officials with the requisite knowledge and skills necessary to address the evolving cyber threats and ensure the security of our vital digital platforms. By fostering a culture of cybersecurity awareness and best practices, sensitive data can be protected and the trust and confidence of the public in digital services can be enhanced.

……