GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION. NO. 3122
TO BE ANSWERED ON: 19.03.2025

BUG 'FREE VIRUS'

3122. SHRI ESWARASAMY K:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether it is a fact that a sophisticated bug ‘free virus’ has infected some highly sensitive installations in the country;
(b) if so, the details thereof; and
(c) the steps taken by the Government to tackle the problem of bug ‘free virus’ and protection of sensitive installations in the country?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) and (b): As per section 70B of the Information Technology Act, 2000, the Indian Computer Emergency Response Team (CERT-In) is the national agency for coordination of cyber security incident response activities. CERT-In receives inputs from its situational awareness systems and threat intelligence sources about malware infections and vulnerabilities in networks of entities across sectors and issues alerts to concerned organisations and sectoral Computer Security Incident Response Teams (CSIRTs) for remedial measures. As per section 70A of the Information Technology (IT) Act, 2000, the Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country. As per NCIIPC, no such incident has been reported for notified Critical Information Infrastructures.

(c): Government has taken following measures to enhance the cyber security posture and prevent cyber attacks including malware attacks:

(i) Cyber Swachhta Kendra (CSK) is a citizen-centric service provided by CERT-In which extends the vision of Swachh Bharat to the Cyber Space. Cyber Swachhta Kendra is the Botnet Cleaning and Malware Analysis Centre that helps to detect malicious programs and provides free tools to remove the same. It also provides cyber security tips and best practices for citizens and organisations.

(ii) CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on an ongoing basis.

(iii) CERT-In operates an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

(iv) National Cyber Coordination Centre (NCCC) implemented by the CERT-In serves as the control room to scan the cyberspace in the country and detect cyber security threats. NCCC facilitates coordination among different agencies by sharing with them the metadata from cyberspace for taking actions to mitigate cyber security threats.

(v) CERT-In issued Cyber Security Directions in April 2022 under sub-section (6) of section 70B of Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

(vi) CERT-In has issued guidelines on information security practices for Government entities in June 2023 covering domains such as data security, network security, identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.

(vii) CERT-In has issued Guidelines for Secure Application Design, Development, and Implementation & Operations in September 2023. CERT-In has also released the Software Bill of Materials (SBOM) guidelines for entities, particularly those in the public sector, government, essential services, organizations involved in software export and software services industry in October 2024. SBOM helps organizations know exactly what components are in their software or assets, making it easier to identify and fix vulnerabilities.

(viii) CERT-In has formulated a Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism for implementation by all Ministries and Departments of the Central Government, State Governments and their organisations and critical sectors.

(ix) CERT-In has empanelled 200 security auditing organisations to support and audit implementation of Information Security Best Practices.

(x) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 109 such drills have so far been conducted by CERT-In where 1438 organizations from different States and sectors participated.

(xi) CERT-In conducts regular training programmes for network and system administrators and Chief Information Security Officers of government and critical sector organisations regarding securing information technology infrastructure and mitigating cyber-attacks. A total of 12,014 officials have been trained in 23 training programs in 2024.

****