GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3624
TO BE ANSWERED ON: 07.12.2016

CERT-IN

3624 DR. SANJAY JAISWAL:

Will the Minister of Electronics & Information Technology be pleased to state:-

(a) whether the Government has taken or proposes to take any steps to strengthen Cert-IN;
(b) if so, the details thereof along with the funds allocated for the purpose; and
(c) the other measures taken to counter the cyber threat?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI P.P. CHAUDHARY)

(a) and (b): The Indian Computer Emergency Response Team (CERT-In) has been designated as the nodal agency for responding to cyber security incidents in the country. CERT-In is operating an incident response help desk, issuing alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures, conducting training programs on specific areas of cyber security and conducting mock drills. In order to deal with emerging threat landscape and to implement new initiatives of the Government to enhance cyber security posture, Government has taken initiatives to strengthen the infrastructure and manpower of CERT-In. An amount of □35 Crores has been allocated to CERT-In for the year 2016-17. Further, Ministry of Finance has approved creation of 20 new posts for Botnet Cleaning Centre under CERT-In and revival of 26 deemed abolished posts.

(c) : Government has taken the following steps to counter cyber threats:

i. The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published guidelines for securing IT infrastructure, which are available on its website (www.certin.org.in). In order to detect variety of threats and imminent cyber attacks from outside the country, periodic scanning of cyber space is carried out.

ii. Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State/UT Governments and their organizations and critical sectors. The Crisis Management Plan is updated periodically on annual basis to take into account changing scenario of cyber threat landscape. Regular workshops are conducted for Ministries, Departments, States & UTs and critical organizations to sensitize them about the cyber security threat landscape and enabling them to prepare and implement the Cyber Crisis Management Plan. So far 41 workshops have been conducted.

iii. Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. So far 11 such drills have been conducted by CERT-In where 110 organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space and IT/ITeS participated.

iv. Government has empaneled security auditing organisations to support and audit implementation of Information Security Best Practices. Currently, 57 organisations have been empaneled.

v. Operationalising the National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the Information Technology Act 2000, for protection of Critical Information Infrastructure in the country. NCIIPC is providing tailored advisories on software/hardware vulnerabilities and alerts on cyber attacks are being issued regularly to Chief Information Security Officers of Critical Information Infrastructure organizations. In addition policy, audit and compliance reports of Critical Information Infrastructure organizations are being analysed.

vi. Government has taken steps toward establishment of Botnet Cleaning and Malware Analysis Centre to detect and clean infected systems in the country. The centre is initiated in coordination with the Internet Service Providers and Industry.

vii. Government is setting up National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

viii. Government is implementing 'Information Security Education and Awareness (ISEA)' project to train professionals / government officials and create mass information security awareness among citizens. The Project is implemented by 51 institutions across the country. So far, 11,110 persons have been trained/undergoing training in various formal/non-formal courses focusing on Cyber Security. 2,384 Government personnel have been trained in direct training programs. C-DAC Hyderabad has conducted 377 Awareness workshops for various user groups covering 42,379 participants from 22 States/UT.

ix. CERT-In is conducting cyber security trainings for IT / cyber security professionals including Chief Information Security Officers (CISOs) of Government and critical sector organisations. As of 31st October, 14 such training programs have been conducted covering 431 participants during the year 2016.

x. Government has set up cyber forensic training & investigation labs for training officers of Law Enforcement and Judiciary. More than 1250 police officers in North Eastern states have been trained. In addition, National Institute of Technical Teachers Training and Research(NITTTR), Chandigarh has trained 2756 Engineering and Polytechnic college teachers, whereas National Law School of India University (NLSIU), Bangalore imparted training to 1398 officials including judiciary, law teachers & practitioners, law students, law researchers, etc.

xi. Government is carrying out Research & Development in the area of Cyber Security for creating cyber security eco-system in the country. It is aimed at development/enhancement of skills and expertise in areas of cyber security by facilitating basic research, technology demonstration and proof-of-concept and R&D test bed projects. Research and development is carried out in the thrust areas of cyber security including cryptography and cryptanalysis, Network & System Security, etc. through sponsored projects at recognized R&D organisations. Currently 32 projects are being pursued to cater to a variety of requirements of Government, Law Enforcement and security agencies, specifically addressing the need of availability as well as development of trustworthy products and solutions.

****