GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2506
TO BE ANSWERED ON: 16.03.2018

**MECHANISM TO GUIDE AND FUND STATE GOVERNMENTS
FOR SECURITY OF DIGITAL DATA**

2506.   DR. T. SUBBARAMI REDDY:

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

(a) whether it is a fact that the number of cyber crime cases in the country have increased
manifold during the last three years;

(b) if so, the details thereof;

(c)   whether Government has any mechanism to guide and fund State Government to
ensure security of digital data, if so, the details thereof; and

(a)   the details of measures taken to guard against external cyber attacks and the money
spent over the last three years in this regard?

ANSWER

MINISTER OF STATE FOR   ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI K. J. ALPHONS)

(a)   and (b): With the proliferation of Information Technology and related services, there
is a rise in instances of cyber crimes in the country like elsewhere in the world. As per the
data maintained by National Crime Records Bureau (NCRB), a total of 9622, 11592 and
12,317 cyber crime cases were registered during the years 2014, 2015 and 2016
respectively.

(c) and (d): Ministry of Electronics & Information Technology (MeitY) does not have any
specific mechanism to fund State Government to ensure security of digital data.

Further, Government has taken following steps to prevent cyber attacks and enhance cyber
security:

(i) Government has set 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. Phase-I of NCCC has already been made operational. To
ensure security of digital data hosted in some State Data Centres (SDC), meta-data
of the security devices of SDCs are analysed at National Cyber Coordination

Centre (NCCC) and necessary actions are taken to mitigate the security risks including advisories to the SDCs.

(ii) Ministry of Electronics & IT (MeitY) has formulated a Cyber Crisis Management Plan (CCMP) for countering cyber-attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors. Several guideline documents and templates have been published to assist development and implementation of sectoral Crisis Management Plans. CERT-In is providing support to Central Government Ministries/Departments and State Governments in preparing their CCMP document. Till now CERT-In has enabled 19 Central Ministries/Departments to develop their own CCMP and interacted with 21 Central Ministries/Departments for CCMP development. 11 states/UTs have been enabled to develop the CCMP and interaction is in process with 14 other states/UTs.

(iii) CCMP workshops are regularly organized by CERT-In for various Central Government Ministries / Departments and States/ UTs to assist them in drawing up their own sectoral Cyber Crisis Management Plans and organizational level Cyber Crisis Management Plans. Till date 54 such workshops are conducted.

(iv) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis.

(v) Cyber security exercises are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 25 such exercises have so far been conducted by CERT-In wherein organisations from different sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS etc participated.

(vi) Government has empanelled 67 security auditing organisations to support and audit implementation of Information Security Best Practices.

(vii) CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. 22 training programs covering 610 participants were conducted during the year 2017.

(viii) Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same.

MeitY had a budget of Rs. 62.0 crores, Rs. 85.0 crore and Rs. 53.6 crore during the years 2014-15, 2015-16 and 2016-17 respectively for cyber security.

******