GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO. 3714
TO BE ANSWERED ON: 09.08.2017

CERT RESPONSE

3714 SHRI DINESH TRIVEDI:

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

(a) whether as per in Rule 12 (a) of the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013, there are two different standards for an individual, organisation or corporate entity on the one hand and intermediaries, service providers, data centre and body corporate on the other;
(b) if so, the details thereof and the reasons therefor; and
(c) whether the Government plans to strengthen this provision by introducing a specific period of time to enable better enforcement of the law.

ANSWER

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

(a) and (b): The constituency of Indian Computer Emergency Response Team (CERT-In) is Indian cyber community. The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 provide for reporting of incidents based on the severity and impact of the incidents. Rule 12 of these Rules deals with reporting of incidents including mandatory reporting of certain incidents as early as possible. While everyone is expected to report the incidents, there are additional obligations on certain organisations like service providers, intermediaries, data centres and body corporate which are considered to have larger impact on public or critical infrastructure. The Rules, nevertheless provide for mandatory reporting of the following kinds of incidents by all as early as possible to minimise the damage, namely:-

- Targeted scanning/probing of critical networks/systems;
- Compromise of critical systems/information;
- Unauthorized access of IT systems/data;
- Defacement of website or intrusion into a website and unauthorized changes such as inserting malicious code, links to external websites, etc.;
- Malicious code attacks such as spreading of virus/worm/Trojan/botnets/spyware;
- Attacks on servers such as database, mail, and DNS and network devices such as routers;
- Identity theft, spoofing and phishing attacks;
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks;
- Attacks on critical infrastructure, (SCADA) Supervisory Control And Data Acquisition systems and wireless networks;

- Attacks on applications such as e-governance, e-commerce, etc.

(c) : While reporting of incidents is expected to be done as early as possible, the Rules are generic in nature. Domain specific timelines are determined by the specific sectors. For instance, banks have already been mandated to report cyber security incidents to Reserve Bank of India and CERT-In within two to six hours.

****