GOVERNMENT OF INDIA
ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:1704
ANSWERED ON:27.07.2016
Critical National Infrastructure
Maadam Smt. Poonamben Hematbhai;Pala Shri Vincent H

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

(a) whether the Government is aware that the UK Government is likely to provide security agencies with the license to hack into electronic devices of an entire town anywhere in the world;
(b) if so, the details thereof;
(c) whether the Critical National Infrastructure of the country in India have adequate protections for safeguard from such hacking and if so the details thereof;
(d) whether the Government has evaluated / proposes to evaluate the challenges likely to be faced by India and the challenges it will impose on individual privacy; and
(e) if so, the details thereof?

Answer

(a) and (b): As per the information available in the public domain, the Investigatory Powers Bill (also known as Snoopers' Charter) is a Bill of the Parliament of the United Kingdom currently undergoing legislative scrutiny. The Bill was introduced in Nov. 2015, to strengthen the operation and regulation of investigatory powers to law enforcement and intelligence agencies, in particular the interception of communications and communications data. For certain defined operations such as acquisition and use of bulk personal datasets, warrants authorized by Secretary of State and approved by Judicial Commissioner are required. The draft Bill proposed obligations on all Communications Service Providers providing services to the United Kingdom or in control of communications systems in the United Kingdom. However, the draft Bill proposed these obligations to be enforced through the courts against overseas companies in respect of communications data acquisition and interception power. The requests for overseas interceptions qare to be administered in accordance with international Mutual Assistance agreement.

(c), (d) and (e): To protect Critical National Infrastructure, Government has taken steps to put in place a Framework for Enhancing Cyber Security, with a multi-layered approach for ensuring defence-in-depth. The salient features of the Framework include setting up institutions and mechanisms for enhancing cyber security, strengthening of assurance and certification framework, promoting R&D and indigenization and engagement with private sector on cyber security. Specific steps relate to actions such as periodic scanning of cyber space and a close watch on critical infrastructure networks to detect variety of threats and imminent attacks; training of manpower engaged in operation of critical networks to protect their systems and networks; conducting mock cyber security drills involving critical sector organizations and providing a platform for the personnel of critical sector organizations to share their experience. In order to enhance the cyber security posture of the Critical infrastructure and improve the ability to resist cyber attacks the following key actions are being pursued:

Further Government has established 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, best practices, controls and guidelines are 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 analysed.

Reserve Bank of India has put in place a robust cyber security / resilience framework at Banks to ensure adequate cyber security preparedness among banks on a continuous basis. The framework includes improving the current defences in addressing cyber risks, putting in place and adaptive incident response, management and recovery framework to deal with adverse incidents / disruptions, if and when they occur. CERTs have been set up by National Thermal Power Corporation (NTPC) and National Hydro Electric Power Corporation (NHPC) and Power Grid Corporation of India (PGCIL).

To address the individual privacy concerns, Government has initiated actions to enhance its capacity to protect data and information flows by building better cyber and telephony infrastructure and by evolving new cyber and telecom security practices. Government is also promoting Indian players in the IT field to develop and offer Internet Services by having the servers located in India, in order to protect the interests and secrecy of communication of Indian citizens. Further Government has taken up the concerns of privacy with International fora for promoting the evolution of better international Internet Governance − norms, through ongoing discussions for addressing the challenges on privacy concerns of individuals. In this direction, India has been actively involved in the deliberations of United Nations Group of Governmental Experts (UNGGE) on developments in the field of information and telecommunications in the context of International security with focus on rules and principles of responsible behaviour by States. Also provisions of the Information Technology Act, 2000 provides comprehensive legal framework for privacy and Security of data in digital form.

****