GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:334
ANSWERED ON:25.02.2015
APPREHENSION OF CYBER ATTACK ON NUCLER PLANTS
Chandel Kunwar Pushpendra Singh

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

(a) whether there is apprehension about probable cyber attacks on nuclear plants in the country;

(b) if so, the details thereof;

(c) whether Indian Security agencies are equipped to safeguard the nuclear plants from such cyber attacks; and

(d) if so, the details thereof and the future action plan prepared by the Government to tackle the cyber threats?

Answer

MINISTER FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI RAVI SHANKAR PRASAD)

(a) and (b): Cyber space and related technologies are characterized by rapid developments. With every Infor- mation Technology (IT) product introduced into the market, newer vulnerabilities are discovered, leaving scope for malicious actions. Probing of systems connected to In- ternet by adversaries to find vulnerable systems is a continuous phenomenon. In tune with the dynamic nature of Information Technology, continuous efforts are re- quired to be made to detect, prevent and recover from cyber attacks. As such, the protection of India`s IT infrastructure in general and critical information infrastructure including nuclear sector in particular is a dynamic activity and continuing process.

(c): Government is aware of the nature of the threats in Cyber Space and accordingly, Government is following an integrated approach with a series of legal, technical and administrative steps to ensure that necessary systems are in place to address the growing threat of cyber attacks in the country.

The Government has taken following steps to enhance cyber security of Critical Information Infrastructure:

i) Security agencies in nuclear installations are backed by technical support to prevent, and safeguard against cyber threats. All software installed and used in nuclear plants are subjected to a system of verification and validation to check software codes in detail. After insta- llation and deployment, physical security measures are taken to protect codes from tampering. Measures are taken to ensure air gap between critical systems and other networks/Internet. Periodic audits are carried out to ensure strict procedures and systems are in proper order and working as per specification.

ii) The Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors including Nuclear sector.

iii) Government has setup National Critical Information Infrastructure Protection Centre (NCIIPC) to protect the critical information infrastructure in the country

iv) Indian Computer Emergency Response Team (CERT-In) is conducting mock cyber security drills to enable assessment of preparation of organizations to withstand cyber attacks. Organisations from Nuclear sector participated in the drills.

v) CERT-In issues the alerts advisories regarding latest Cyber threats and counter measures.

vi) CERT-In has empanelled information security auditors through a stringent mechanism of selection to carryout audits.

vii) The Government has circulated Computer Security Policy and Guidelines to all the Ministries/Departments on taking steps to prevent, detect and mitigate cyber attacks.

(d): Government has released the "National Cyber Security Policy − 2013" for public use and implementation with all relevant stakeholders. Its stated mission is "to protect information and information infrastructure in cyber space, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation`. It seeks to do so by creating a secure cyber ecosystem and an assurance framework, encouraging open standards, strengthening the regulatory framework, vulnerability management, promotion of research and development in cyber security and enhancing our technical skill sets and human resources. Actions on the components

of the Policy are to be taken by Government, Public and Private sector.

The Framework for Enhancing Cyber Security, envisages a multi-layered approach for ensuring defence-in-depth with clear demarcation of responsibilities among the stakeholder organizations in the country. 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 indigeni- zation, human resource development and engagement with private sector on cyber security.