GOVERNMENT OF INDIA
DEPARTMENT OF ATOMIC ENERGY
LOK SABHA
UNSTARRED QUESTION NO.1007
TO BE ANSWERED ON 08.02.2017

CYBER ATTACK ON NUCLEAR INSTALLATIONS

1007. SHRI PRAHLAD SINGH PATEL:

Will the PRIME MINISTER be pleased to state:

(a) whether our nuclear establishment including nuclear power plants are well prepared to withstand any cyber attack;

(b) if so, the details thereof including the number of cyber attacks targeting the nuclear establishments during the last three years in the country;

(c) whether the Government periodically conducts cyber network capability test to check the cyber attacks on the nuclear establishments in the country;

(d) if so, the details thereof and if not, the reasons therefor; and

(e) the steps taken/proposed to be taken by the Government in this regard ?

ANSWER

THE MINISTER OF STATE FOR PERSONNEL, PUBLIC GRIEVANCES & PENSIONS AND PRIME MINISTER'S OFFICE (Dr. JITENDRA SINGH) :

(a) Yes, Sir.

(b) Indian nuclear establishment's plant control systems/electronic systems are designed and developed in-house using custom built hardware and software which are subjected to regulatory verification and validation, thereby making it immune to cyber security threats. Critical infrastructure of Indian nuclear establishment is isolated from Internet.

Department of Atomic Energy (DAE) has specialist groups like Computer and Information Security Advisory Group (CISAG) and Task force for Instrumentation and control security (TAFICS) to look after cyber security/information security of DAE units.

…2

Cyber space is being continuously scanned by hackers to detect vulnerable systems which can be exploited to breach organization's network. DAE sees these attempts in large numbers (e.g. Bhabha Atomic Research Centre (BARC), a unit of DAE sees scanning attempts in several thousands per day). DAE has strong cyber security infrastructure which is regularly updated and audited. During last 3 years, no breaches have been reported in DAE's nuclear establishments.

(c),(d)&(e) All DAE units conduct quarterly cyber security audit of their cyber infrastructure and submit reports to CISAG (Computer & Information Security Advisory Group) of DAE. CISAG, DAE also forms teams of experts drawn from various units of DAE and performs cyber security audit of DAE units. DAE also engages services of Standardisation Testing and Quality Certification (STQC) of Ministry of Electronics and Information Technology to test its systems/networks which are connected to internet to identify vulnerabilities, if any. Any weakness reported is addressed immediately. DAE also participates in drills conducted by CERT-In (Computer Emergency Response Team) of India to gauge preparedness of organizations to face cyber attacks. In such drills, DAE's performance has been found to be excellent.

****