GOVERNMENT OF INDIA
MINISTRY OF POWER

LOK SABHA
UNSTARRED QUESTION NO.4890
TO BE ANSWERED ON 25.03.2021

PROTECTION OF POWER GRID FROM CYBER ATTACK

4890. SHRI PARVESH SAHIB SINGH VERMA:
SHRI SUDHAKAR TUKARAM SHRANGARE:
SHRI RAVNEET SINGH BITTU:
MS. PRATIMA BHOUMIK:
SHRI PRADEEP KUMAR SINGH:
SHRI SUMEDHANAND SARASWATI:
SHRI UTTAM KUMAR REDDY NALAMADA:
SHRI PRATHAP SIMHA:
SHRI BHAGWANTH KHUBA:
SHRI SYED IMTIAZ JALEEL:
SHRI ASADUDDIN OWAISI:
SHRI D.M. KATHIR ANAND:

Will the Minister of POWER be pleased to state:

(a) whether the Government has conducted any study to identify the vulnerabilities of the energy supply grid in the country to cyber attacks;

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

(c) the number and details of cyber attacks on the power grid and the cases and sources of malware found in the energy supply system during the last two years and the current year;

(d) whether some States faced electricity blackout or massive power outrage due to the said cyber attacks that manage power supply across the country and if so, the factual position in this regard;

(e) whether the Government has carried out any investigation in this regard along with the measures taken/being taken to ensure the safety of the power grids from such cyber attacks in future;

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

(g) whether the Government proposes to set up a team to oversee cyber security of the energy supply infrastructure in the country and if so, the details thereof?

A N S W E R

THE MINISTER OF STATE (INDEPENDENT CHARGE) FOR POWER, NEW & RENEWABLE ENERGY AND THE MINISTER OF STATE FOR SKILL DEVELOPMENT & ENTREPRENEURSHIP

(SHRI R.K. SINGH)

(a) & (b) : As per the Information Technology Amendment Act 2008, Indian Computer Emergency Response Team (CERT-In) has been designated as National Agency to collect, analyse and disseminate the information on cyber incidents in the country. CERT-In also issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers

.....2.

and networks on regular basis. Further, as per the provisions of section 70A of the Information Technology (IT) Act, 2000, Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country. Ministry of Power (MoP) has established Sectoral Computer Emergency Response Teams (CERTs)- viz. CERT-Thermal, CERT-Hydro, CERT-Distribution, CERT-Trans, CERT-Grid Operation etc. to strengthen the power system in the country so that cyber attacks are not able to disrupt it, and to promptly detect and counter any attempt of cyber attack on our systems.

(c) : In the recent past, cyber incidents have been reported at Southern Region Load Despatch Center (SRLDC), Western Region Load Despatch Center (WRLDC) and North Eastern Region Load Despatch Center (NERLDC) of Power System Operation Corporation (POSOCO), NTPC Kudgi and Telangana State Transco. Necessary isolation and other protection measures have been taken by these organizations. Further detailed analysis of the incidents is under process under the guidance of CERT-In.

(d) : No, Sir.

(e) & (f) : The incidents of cyber attacks have been investigated. Further investigations and analysis are in progress. Government has taken following measures to enhance the cyber security posture and prevent cyber attacks:

i. **The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding the latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on a regular basis.**

ii. **Government has issued guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications / infrastructure and compliance.**

iii. **All the Government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications will be conducted on a regular basis after hosting also.**

iv. **Government has empanelled security auditing organisations to support and audit implementation of Information Security Best Practices.**

v. **Government has formulated Cyber Crisis Management Plan (CCMP) for countering cyber attacks for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.**

vi. **Cyber security mock drills are being conducted regularly in Government and critical sectors.**

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.**

viii. **Government is operating 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.**

.....3.

ix. **Government has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats. Phase-I of NCCC is operational.**

(g) : At the level of Ministry of Power (MoP), a committee has been constituted in March 2017 to look into the issue of Power firms seeking to enter Indian Power Transmission Sector and related issues of cyber security. Subsequently, a committee was set up in August 2019 to examine ways and means to enhance cyber security in our transmission systems.

In addition to above, a Group of Officers (GoO) was set up in March 2020 to study the contractual and legal issues in connection with cyber-attack in power sector. The report of the committee has been received and it is under examination/deliberation for taking steps to further strengthen cyber security in power sector. In September 2020, a committee has been constituted for deciding designating laboratories and testing protocols for imported equipment.

Recently, MoP has constituted an Empowered Committee under the chairmanship of Secretary (Power) and a Standing Committee under the chairmanship of Additional Secretary (Power) to review the cyber security preparedness of power sector.

MoP has also requested the States/UTs for various action to be taken to protect the power system equipment in their respective State/UT.

Further, to protect the security, integrity and reliability of the strategically important and critical Power Supply System & Network in the country, the following directions have been issued:-

(i) All equipment, components, and parts imported for use in the power Supply System and Network shall be tested in the country to check for any kind of embedded malware/trojans/cyber threat and for adherence to Indian Standards.

(ii) All such testings shall be done in certified laboratories designated by the MoP.

(iii) Any import of sensitive equipment/components/parts for critical transmission system from "prior reference" countries as specified or by persons owned by, controlled by, or subject to the jurisdiction or the directions of these "prior reference" countries will require prior permission of the Government of India.

(iv) Where such sensitive equipment/components/parts are imported from "prior reference" countries, with special permission, the protocol for their testing in certified and designated laboratories shall be approved by the MoP.

****