GOVERNMENT OF INDIA
MINISTRY OF POWER
LOK SABHA
UNSTARRED QUESTION NO.1916
ANSWERED ON 28.07.2022

ENERGY SUPPLY GRID

1916. DR. SUJAY RADHAKRISHNA VIKHEPATIL:
DR. HEENA GAVIT:
PROF. RITA BAHUGUNA JOSHI:
DR. SHRIKANT EKNATH SHINDE:
DR. KRISHNA PAL SINGH YADAV:

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 during the last three years and the current year;

(b) if so, the details thereof and if not, the reasons therefor, State/UT-wise;

(c) whether the Government has carried out any investigation in this regard along with the measures taken/being taken to ensure the safety of the powergrids from cyber-attacks in future; and

(d) if so, the details thereof and if not, the reasons therefor, State/UT-wise?

ANSWER

THE MINISTER OF POWER AND NEW & RENEWABLE ENERGY

(SHRI R.K. SINGH)

(a) to (d) : Ministry of Power vide order No. 9/16/2016-Trans dated 05.08.2019 had constituted a committee to examine whether the presence of some of the equipment of foreign make in the transmission System makes it vulnerable particularly for the perspective of security of the grid. Further, MoP vide order No. 9/16/2016-Trans dated 03.02.2020 constituted Group of Officers (GOO) to study contractual and related legal issues in Cyber Supply Chain Mechanism.

Based on various recommendations, various measures have been taken by the Central Government to ensure the safety of the Indian power grids from cyber-attacks which are given at Annexure.

****

ANNEXURE

ANNEXURE REFERRED TO IN REPLY TO PARTS (a) TO (d) OF UNSTARRED QUESTION NO. 1916 ANSWERED IN THE LOK SABHA ON 28.07.2022

****

(i) Under the provisions of section 70A of the Information Technology (IT) Act, 2000, the Central Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country. NCIIPC provides near real-time threat intelligence and situational awareness based on which regular alerts and advisories are sent to Critical Information Infrastructure (CII)/ Protected System (PS) entities.

(ii) Government of India, under the provisions of section 70B of the Information Technology Act, 2000, has established the Indian Computer Emergency Response Team (CERT-In) and designated as the national agency for responding to cyber security incidents. CERT-In is operating an automated cyber threat exchange platform for proactively collecting, analyzing and sharing tailored alerts with Power Sector Utilities for proactive threat mitigation actions by them.

(iii) CERT-In is operating the Cyber Swachhta Kendra (CSK) (Botnet Cleaning and Malware Analysis Centre). The CSK is providing free tools developed in collaboration with industry and research institutions for detection and removal of malicious code and securing computers and mobile devices. MoP has mandated all power Sector utilities to on board CSK of CERT-In. Regular alerts and advisories regarding latest cyber threats/vulnerabilities and include the details of MoP order dated 02.09.2020 of counter measures to protect networks are issued on regular basis.

(iv) Central Electricity Authority has recently issued CSPS (Cyber Security in Power Sector), Guidelines, 2021 detailing the mandatory requirements e.g.

a. Cyber Security Audit of IT and OT system by the CERT-In empanelled auditors once in every six months.

b. Critical Information Infrastructure (CIIs) to be identified in co-ordination with NCIIPC.

c. Cyber Crisis Management Plan (CCMP) to be prepared and vetted by CERT-In

d. Implementation of ISMS/ISO 27001.

e. Cyber security mock drills to be conducted regularly

f. Cyber Security training from the Training Institutes designated by CEA for all IT/OT personnel

(v) Ministry of Power had constituted six Sectoral CERTs namely CERT-Thermal, CERT-Hydro, CERT-Transmission, CERT-Distribution, CERT-Grid Operation and CERT-Renewable Energy to coordinate and monitor the cyber security issues with concerned power utilities. These sectoral CERTs monitor the implementation of various Cyber security measure as mandated in CEA (Cyber Security in Power Sector), Guidelines, 2021.

(vi) MoP has setup up a dedicated body i.e. Computer Security Incident Response Team (CSIRT) for Power sector to be housed at CEA.CSIRT will coordinate and support the response to cyber security incidents. It will provide services and support to its constituent utilities for preventing, detecting, handling, and responding to cyber security incidents CSIRT-Power will help to mitigate and prevent major incidents and to protect valuable assets and deliver services effectively. For proper functioning of CSIRT-Power, a Security Operation Center (SOC) is envisaged.

(vii) To ensure cyber security during procurement of Information and Communication Technologies (ICT) based component/equipment/system for use in Power Supply System, a scheme for identification of Trusted Sources and Trusted Vendor is envisaged.

(viii) CERT-In conducts regular training programmes for *Chief Information Security Officers* (*CISOs*) of all utilities of Power Sectors for securing the Information Technology (IT) and Operational Technology (OT) infrastructure and mitigating cyber-attacks. Cyber security mock drills in co-ordination with CERT-In are being conducted regularly in utilities of Power Sectors.

(ix) Curriculum for Basic, Intermediate advance level cyber security has been worked out by Central Electricity Authority(CEA) and National Power Training Institute (NPTI) and courses are being conducted regularly at NPTI for all load dispatchers of Regional Load Despatch Centres (RLDCs) and State Load Despatch Centres (SLDCs) and other IT/OT person of power sector utilities.

(x) Further, National Cyber Testing Lab at Central Power Research Institute (CPRI) Bengaluru to implement the MoP order dated 02.07.2020 on testing power system equipment for use in the Supply System and Networks in the country for cyber security, work on all associated activity like designating Testing labs, and Testing protocols to be followed, etc. are taken up on high priority.

****