

**GOVERNMENT OF INDIA  
MINISTRY OF POWER  
LOK SABHA  
UNSTARRED QUESTION NO.1273  
ANSWERED ON 27.07.2023**

**SAFETY OF NATIONAL POWER GRID**

**1273. SHRI SHANMUGA SUNDARAM K.:**

**Will the Minister of POWER  
be pleased to state:**

- (a) the details of the functional operability of National Power Grid;**
- (b) whether the Government has taken sufficient steps to protect the National Power Grid from Cyber attacks and if so, the details thereof;**
- (c) if not, the reasons therefor;**
- (d) the details of cyber attacks taken place on the National Power Grid, year-wise since 2014;**
- (e) whether such entities involved in cyber attacks on the power grid are prosecuted and punished and if so, the details thereof; and**
- (f) if not, the reasons therefor?**

**A N S W E R**

**THE MINISTER OF POWER AND NEW & RENEWABLE ENERGY**

**(SHRI R.K. SINGH)**

**(a): The Indian national power grid serves the Generators, Transmission, Distribution systems and the consumers of the electricity. The Indian grid is demarcated into 5 synchronously connected regional grids viz. Northern Region, Eastern Region, North Eastern Region, Southern Region and Western Region which also encompass the state grids in respective regions. The supervision of power grid and coordination with different utilities is being carried out by the National Load Despatch Centre (NLDC) and respective Regional Load Despatch Centres (RLDC) and State Load Despatch Centres (SLDC) as per their jurisdiction at various hierarchical level at national, regional and state.**

**(b) & (c): Government of India has taken following steps to protect the National Power Grid from Cyber attacks:**

- Central Electricity Authority (CEA) has issued Guidelines for Cyber security in Power Sector in October 2021 leading to development and implementation of Cyber Security measures such as Cyber Crisis Management Plans, identification of Critical Information Infrastructures,**

**Information Security Management System (ISO 27001), Onboarding Cyber Swatchatta Kendra of Indian Computer Emergency Response Team (CERT-In) for monitoring open & vulnerable services and botnet infections, vulnerability assessment of critical installations through CERT-In empaneled auditors, skill enhancement of workforce through level 1& 2 training conducted by National Power Training Institute (NPTI).**

- **A Computer Security Incident Response Team for Power sector (CSIRT-Power) under guidance of CERT-In has been setup at CEA, to coordinate and support the response to cyber security incidents and hand-hold utilities for preventing, detecting, handling, and responding to cyber security incidents. CSIRT-Power provides expert guidance to mitigate and prevent cyber incidents to protect Critical Information Infrastructure assets and enhance cyber resilience.**
- **As Computer Emergency Response Team of Grid Operations, Grid-India, apart from taking care of cyber security of RLDC(s) and NLDC control centres, also coordinates with SLDCs for taking care of cyber security of their respective control centre by them.**
- **The IT (Information Technology) and OT (Operation Technology) systems of NLDC/RLDCs under GRID-INDIA has been designed considering necessary controls to mitigate the cyber threats and associated cyber security devices have been installed for prevention of cyber-attacks.**
- **The coordination with the statutory bodies and compliance to the directives thereof are ensured by GRID-INDIA on regular basis.**
- **Establishment of Security Operations Center (SOC) and on boarding with Cyber Swachhta Kendra (CSK): GRID-INDIA has established a 24x7 Security Operations Center.**
- **Employee awareness sessions are being conducted frequently to sensitize employees about cyber security.**
- **Mandatory Cyber Security Certification through NPTI have been introduced for IT /OT and cyber security personnel of GRID-INDIA**

**(d) : As informed by POWERGIRD and GRID-INDIA, there has been no Cyber attack on their systems since 2014.**

**(e) & (f) : Does not arise in view of (d) above.**

\*\*\*\*\*