# GOVERNMENT OF INDIA
# POWER
# LOK SABHA

STARRED QUESTION NO:177
ANSWERED ON:02.12.2011
SAFETY OF POWER GRIDS
Suvendu Shri Adhikari

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

(a) the details of the technological systems, including Real Time Despatch, available at Load Centres, to monitor frequency of power, at a given time;

(b) whether the Union Government is giving due cognizance to secure power grids and other installations from being hacked online through embedded malware (malicious software);

(c) if so, the details thereof;

(d) the instances of such hackings reported during the last one year and the current year; and

(e) the steps taken or proposed to be taken by the Government to prevent recurrence of such incidents?

## Answer

MINISTER OF THE STATE IN THE MINISTRY OF POWER (SHRI SUSHILKUMAR SHINDE)

(a)to(e): A Statement is laid on the Table of the House.

STATEMENT REFERRED TO IN REPLY TO PARTS (a) TO (e) OF STARRED QUESTION NO. 177 TO BE ANSWERED IN THE LOK SABHA ON 02.12.2011 REGARDINGSAFETY OF POWER GRIDs.

(a): Conventional Supervisory Control and Data Acquisition (SCADA)/Energy Management System (EMS) is installed at all five Regional Load Despatch Centres (RLDCs) and National Load Despatch Centre (NLDC) to monitor frequency of power at a given time.

(b)&(c): Yes, Madam. Union Government has given due cognizance to secure its power grids and installations from online hacking through embedded malware.

The details in this regard are as under :

(i) In NLDC and RLDCs, redundancy has been kept in configuration of critical functions and power supply units. Failure of one single server does not affect the whole system.

(ii) The new SCADA/EMS specifications are equipped with atechnological barrier designed to prevent unauthorized access or unwanted communications between sections of a computer network. A firewall inspects network traffic passing through it, and denies or permits passage based on a set of rules. It is normally placed between a protected network and an unprotected network and acts like a gate to protect assets to ensure that nothing private goes out and nothing malicious comes in.

(iii) Another additional feature with respect to security provisions in new specifications is DMZ, or demilitarized zone. It is a physical or logical sub network that contains and safely exposes the system for external services to a larger un-trusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to the system`s Local Area Network (LAN); an external attacker only has access to equipment in the DMZ.

(iv) All the firewall protection is combined with antivirus gateway and Network Intrusion Protection (NIP) along with secured patch management system.

(v) NLDC and RLDCs are also certified for Information Security Management Systems (ISMS) ISO 27001:2005

(d): There is no instance of hacking observed at NLDC and five RLDCs under the supervision of Power System OperationCorporation Limited (POSOCO).

(e): Initiatives taken by Government of India to prevent occurrence of hacking are as under :-

(1) Crisis Management Plan (CMP) for countering cyber attacks and cyber terrorism has been adopted.

(2) Ministry of Power has constituted Sectoral Computer Emergency Restoration Teams (CERTs) for Hydro, Thermal and Transmission.

(3) India Smart Grid Task Force (ISGTF) has been constituted- Working Group No. 5 is addressing cyber security issue of transmission grid.