

GOVERNMENT OF INDIA
DEPARTMENT OF ATOMIC ENERGY
LOK SABHA
UNSTARRED QUESTION NO.3239
TO BE ANSWERED ON 23.03.2022

CYBER SECURITY BREACH IN NUCLEAR PLANTS

3239. SHRI PRATAP CHANDRA SARANGI:
SHRI MAHENDRA SINGH SOLANKY:
SHRI MANOJ TIWARI:
SHRI RAM KRIPAL YADAV:
SHRI SANGAM LAL GUPTA:
SHRI CHANDRA PRAKASH JOSHI:
SHRI RAJBAHADUR SINGH:
SHRI BRIJBHUSHAN SHARAN SINGH:

Will the PRIME MINISTER be pleased to state:

- (a) whether the Government is aware of the growing challenges of cyber security breaches in nuclear facilities across the world;
- (b) if so, the steps taken by the Government to ensure India's nuclear security infrastructure;
- (c) whether there are any plans to collaborate for technology exchange with the countries that have signed civil nuclear cooperation agreements to create a robust cyber security system and infrastructure; and
- (d) if so, the details thereof and if not the reasons therefor?

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 have set rigorous procedure for design, development and operation of the systems used in its installations. The safety and security critical systems are designed and developed in-house using custom built hardware and software which are subjected to regulatory verification and validation, thereby making them resistant to cyber security threats. Critical infrastructure of nuclear power plant establishment is isolated from Internet and access to such systems is restricted to authorized personnel and is closely monitored. The Department of Atomic Energy (DAE) has

specialist groups viz. Computer and Information Security Advisory Group (CISAG) and Task force for Instrumentation and Control Security (TAFICS) to look after cyber security/information security of NPCIL among other constituent units of DAE, including regular cyber security audit. Several measures have also been taken for further strengthening of Information Security in nuclear power plants viz. hardening of internet and administrative intranet connectivity, restriction on removable media, blocking of websites & IPs.

(c) No, Sir.

(d) The cyber security infrastructure in DAE's facilities/plants follow design principles and guidelines setup by DAE CISAG and India's central cyber security agencies such as CERT-IN. On the plant side, all computer-based systems are based on standards and guidelines formulated by Atomic Energy Regulatory Board and TAFICS which are ultimately derived in large part based on standards established by International Atomic Energy Agency (IAEA).
