GOVERNMENT OF INDIA
DEPARTMENT OF ATOMIC ENERGY
LOK SABHA
UNSTARRED QUESTION NO.669
TO BE ANSWERED ON 20.11.2019

EXPANSION AND SAFETY OF KKNPP

669. SHRIMATI SUPRIYA SULE:
DR. AMOL RAMSING KOLHE:
SHRI SUNIL DATTATRAY TATKARE:
DR. SUBHASH RAMRAO BHAMRE:
SHRI KULDEEP RAI SHARMA:

Will the PRIME MINISTERbe pleased to state:

(a) whether the Government is aware of the recent malware infection at the Kundankulam Nuclear Power Plant (KKNPP) in Tamil Nadu putting the entire nuclear plant at risk and if so, the details thereof;

(b) whether the Government has initiated any investigation in the matter and if so, the details and the outcome thereof;

(c) the other steps taken by the Government for the safety of Nuclear Power Plants in the country;

(d) whether Units I and II of Kundankulam Nuclear Power Plant is operating at their optimum level and the Union Government has approached the State Government of Tamil Nadu to grant permission for further reactor expansion at the Kudankulam Nuclear Power Plant for Unit III and Unit IV; and

(e) if so, the details thereof alongwith the response of the State Government thereto?

ANSWER

THE MINISTER OF STATE FOR PERSONNEL, PUBLIC GRIEVANCES & PENSIONS AND PRIME MINISTER'S OFFICE (DR.JITENDRA SINGH):

(a) Yes, Sir. A malware infection was identified in NPCIL KKNPP Internet connected system. The malware infection was identified on KKNPP administrative network used for day to day administrative activities. The affected system contains data related to administrative function. Plant control and instrumentation system is not connected to any external network such as Intranet, Internet and administrative system. The plant systems, which are isolated and not accessible from this administrative network, were not affected. Thus there was no risk to the nuclear power plant at all.

(b) Investigations have been carried out by the Computer & Information Security Advisory Group (CISAG) – DAE along with the national agency, Indian Computer Emergency Response Team (CERT-In). The investigations concluded that the malware infection was limited to Administrative network of KKNPP.

(c) In nuclear power plant systems, security arrangements are in place which secure the plant from cyber-attack. These security measures include authorization, authentication and access control mechanisms, strict configuration control and surveillance. Additionally, these plant systems are isolated from internet and are not accessible from administrative network.

In respect of further strengthening of Information Security in administrative networks, various measures have been taken viz. hardening of internet and administrative intranet connectivity, restriction on removable media, blocking of websites & IPs which have been identified with malicious activity etc.

CISAG-DAE has recommended certain measures for immediate and short term implementation. These are being complied with.

(d)&(e) The KNNPP Units 1&2 are presently operating at 1000 MW and around 600 MW respectively. Units 3&4 are under construction and have achieved a physical progress of 34.62% as of October 2019. In Units 5&6, ground preparations are underway for start of construction. Various statutory and regulatory permissions / clearances for these units have been obtained. The various works on these units are progressing in accordance with the permissions / clearances received.

*****