

GOVERNMENT OF INDIA
DEPARTMENT OF ATOMIC ENERGY
RAJYA SABHA
STARRED QUESTION NO.*109
TO BE ANSWERED ON 28.11.2019

CYBER ATTACK ON KUDANKULAM NUCLEAR POWER PLANT

*109. SHRI A. K. SELVARAJ:

Will the PRIME MINISTER be pleased to state:

- (a) whether it is a fact that there has been a cyber attack on Kudankulam Nuclear Power Plant;
- (b) if so, the details thereof;
- (c) whether it is also a fact that a cyber security audit had been conducted recently at Kudankulam after a futile attempt to hack the Nuclear Power Corporation of India Limited's (NPCIL) isolated network was made; and
- (d) what are the steps taken by the NPCIL to make sure that all plants are hack proof?

ANSWER

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

(a)to(d) A statement is placed on the Table of the House.

Government of India
Department of Atomic Energy

STATEMENT REFERRED TO IN REPLY TO RAJYA SABHA STARRED QUESTION NO. *109 DUE FOR ANSWER ON 28.11.2019 BY SHRI A. K. SELVARAJ REGARDING CYBER ATTACK ON KUDANKULAM NUCLEAR POWER PLANT.

- (a)&(b) There was an identification of a malware infection on Kudankulam Nuclear Power Plant (KKNPP) administrative network which is used for day to day administrative activities. Plant control and instrumentation system is not connected to any external network such as Intranet, Internet and administrative system and thus was not affected.
- (c) Cyber security audit has been carried out by the Computer & Information Security Advisory Group (CISAG) of DAE along with the national agency, Indian Computer Emergency Response Team (CERT-In). It concluded that the malware infection was limited to the administrative network of KKNPP.
- (d) The CISAG-DAE has recommended certain measures for immediate and short term implementation which are being implemented.

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.
