

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 2325
TO BE ANSWERED ON 17.12.2021

DOMESTIC OPERATING SYSTEM FOR COUNTERING THREATS

2325 SMT. AMBIKA SONI:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:-

- (a) whether Government proposes to create a domestic operating system for itself to boost Government's capabilities to deal with potential internal and external threats;
- (b) if so, the details thereof and if not, the reasons therefor; and
- (c) the steps taken by Government to have a comprehensive framework that addresses national security threats as well as to evolve the infrastructure with latest developments in the technological field?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a) and (b): Yes, Madam. India has developed the domestic variants of Open Source Operating Systems. Ministry of Electronics and Information Technology (MeitY) through CDAC Chennai has been maintaining and supporting the Debian based Bharat Operating System Solutions (BOSS) under National Resource Center for Free and Open Source Software (NRCFOSS) to meet the domestic requirements.

Government of India (GoI) is committed to promote use of Open Source technologies and their adaptation in e-Governance/ Digital Governance applications including public platforms in the country.

(c): Government has set up Indian Computer Emergency Response Team (CERT-In) under Section 70B of the Information Technology Act 2000 (Amended in 2008) for responding to cyber security incidents. CERT-In is designated to serve as National Nodal Agency to respond to cyber incidents. CERT-In issues alerts and advisories regarding latest cyber threats/ vulnerabilities and countermeasures to protect computers and networks on regular basis. CERT-In has also formulated a Cyber Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) as per the provisions of Section 70A of the Information Technology (IT) Act, 2000 for protection of critical information infrastructure in the country. NCIIPC has been regularly advising the critical information infrastructure sector organisations to reduce vulnerabilities to all kinds of threats and attacks by sharing threat intelligence, guidelines, best practices and frameworks for protection and guiding them with policies and protection strategies. In addition, training and awareness programs are regularly conducted to improve the cyber hygiene in critical information infrastructure organisations.
