

(b) how many such cases are pending and what is the average time taken to grant clearance; and

(c) whether security clearances delay FDI in the country?

THE MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS (SHRI G. KISHAN REDDY): (a) and (b) Ministry of Home Affairs makes every endeavour to accord security clearance to cases of Foreign Direct Investment (FDI) expeditiously. The average time taken for clearance of such proposals has reduced significantly from about four months in 2014 to about two months in 2019. Only seven cases of FDI are presently under the consideration of Ministry of Home Affairs and no case is pending beyond prescribed time limit.

(c) No, Sir.

Cyber crime and cyber security

2747. SHRI SHAMSHER SINGH MANHAS: Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether cyber crime and cyber security have national and international dimensions;

(b) whether Government has taken any steps to deal with cyber crime and cyber security; and

(c) if so, the details thereof?

THE MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS (SHRI G. KISHAN REDDY): (a) Yes, Sir.

(b) and (c) 'Police' and 'Public Order' are State subjects as per the Constitution of India. States/UTs are primarily responsible for prevention, detection, investigation and prosecution of crimes through their law enforcement machinery. The Law Enforcement Agencies take legal action as per provisions of law against the cyber crime offenders.

However, Central Government has taken steps to spread awareness about cyber crimes, issue of alerts/advisories, capacity building/training of law enforcement personnel/prosecutors/judicial officers, improving cyber forensics facilities etc. to prevent such crimes and to speed up investigation. The Government has launched the online

cyber crime reporting portal, www.cybercrime.gov.in to enable complainants to report complaints pertaining to Child Pornography/Child Sexual Abuse Material, rape/gang rape imageries or sexually explicit content. The Central Government has rolled out a scheme for establishment of Indian Cyber Crime Coordination Centre (I4C) to handle issues related to cyber crime in the country in a comprehensive and coordinated manner.

Further, Government has taken several steps to prevent and mitigate cyber security incidents. These include:—

- (i) Establishment of National Critical Information Infrastructure Protection Centre (NCIIIPC) for protection of critical information infrastructure in the country.
- (ii) All organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously.
- (iii) Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) has been launched for providing detection of malicious programmes and free tools to remove such programmes.
- (iv) Issue of alerts and advisories regarding cyber threats and counter-measures by CERT-In.
- (v) Issue of guidelines for Chief Information Security Officers (CISOs) regarding their key roles and responsibilities for securing applications/infrastructure and compliance.
- (vi) Provision for audit of the Government websites and applications prior to their hosting, and thereafter at regular intervals.
- (vii) Empanelment of security auditing organisations to support and audit implementation of Information Security Best Practices.
- (viii) Formulation of Crisis Management Plan for countering cyber attacks and cyber terrorism.
- (ix) Conducting cyber security mock drills and exercises regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors.
- (x) Conducting regular training programmes for network/system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks.