GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:4030
ANSWERED ON:05.09.2012
UPGRADATION OF CYBER SECURITY
Adhalrao Patil Shri Shivaji;Adsul Shri Anandrao Vithoba;Balram Shri P.;Das Shri Bhakta Charan;Dharmshi Shri Babar Gajanan;Dhotre Shri Sanjay Shamrao;Gaddigoudar Shri P.C.;Gowda Shri D.B. Chandre;Kalmadi Shri Suresh;Mishra Shri Mahabal ;Shankar Alias Kushal Tiwari Shri Bhisma;Tanwar Shri Ashok;Yadav Shri Dharmendra

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

(a) whether the National Security Council Secretariat (NSCS) has come up with any comprehensive Cyber Security Plan / Policy for upgrading the security of systems and preventing them from being hacked, attacked with malware or intruded upon by hostile entities;

(b) if so, the salient features and the present status thereof;

(c) the names of agencies presently authorized for certification of this network;

(d) whether the Government proposes to create a technical professional body for certifying Security Network;

(e) if so, the modalities thereof along with the role likely to be played by the private agencies in this regard; and

(f) the other measures taken by the Government for prevention of Cyber Attack / Crime including amending the relevant provision of Laws in this regard?

Answer

MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI SACHIN PILOT)

(a) and (b): Ministries / Organizations are taking steps for upgrading the security of systems and Networks in their areas of responsibilities in accordance with Crisis Management Plan. National Security Council Secretariat (NSCS) has proposed a broader framework for Cyber Security Architecture for upgrading the security of National Cyber Space. The proposed architecture addresses the aspects of threat monitoring, assurance & certification, Research & Development and Indigenisation. The proposal is tinder evolution stage.

(c): Agencies in Public and Private Sector provide services for penetration testing and security auditing of Systems and Networks. Indian Computer Emergency Response Team (CERT-In) has empanelled Cyber Security auditing Organizations to provide Information Technology (IT) Security Auditing services to various Organizations for improving the security posture of Networks and Systems.

(d) and (e): The proposal being evolved by National Security Council Secretariat (NSCS) also envisages auditing and certification of security networks.

(f): Various steps have been taken by the Government for prevention of cyber attacks / crimes and enhancing Cyber Security which include the following:

i) Legal framework in the form of Information Technology Act, 2000 to address the issues connected with hacking, security breaches and data protection is in place.

ii) The organizations operating critical information infrastructure are regularly advised to implement information security management practices based on International Standard ISO 27001.

iii) All Central Government Ministries/Departments and State/Union Territory Governments have been advised to conduct security auditing of their entire Information Technology infrastructure including websites periodically to discover gaps with respect to security practices and take appropriate corrective actions.

iv) A `Crisis Management Plan for countering cyber attacks and cyber terrorism` has been prepared and circulated for implementation by all Ministries/Departments of Central Government, State Government and all their organizations and critical sectors.

v) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published security guidelines for securing websites. Training programs for the system/network administrator for securing the websites is carried out by CERT-In on regular basis.