17

STANDING COMMITTEE ON INFORMATION TECHNOLOGY (2015-16)

SIXTEENTH LOK SABHA

(MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY)
DEPARTMENT OF ELECTRONICS AND INFORMATION TECHNOLOGY

[Action Taken by the Government on the Recommendations/Observations of the Committee contained in their Fifty-second Report (Fifteenth Lok Sabha) on 'Cyber Crime, Cyber Security and Right to Privacy']

SEVENTEENTH REPORT

LOK SABHA SECRETARIAT
NEW DELHI

December, 2015/Agrahayana, 1937 (Saka)

SEVENTEENTH REPORT

STANDING COMMITTEE ON INFORMATION TECHNOLOGY (2015-16)

(SIXTEENTH LOK SABHA)

(MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY)
DEPARTMENT OF ELECTRONICS AND INFORMATION TECHNOLOGY

[Action Taken by the Government on the Recommendations/Observations of the Committee contained in their Fifty-second Report (Fifteenth Lok Sabha) on 'Cyber Crime, Cyber Security and Right to Privacy']

Presented to Lok Sabha on 21.12.2015
Laid in Rajya Sabha on 21.12.2015

LOK SABHA SECRETARIAT
NEW DELHI

December, 2015/Agrahayana, 1937 (Saka)

CONTENTS

APPENDICES

COMPOSITION OF THE STANDING COMMITTEE ON INFORMATION TECHNOLOGY (2015-16)

Shri Anurag Singh Thakur - Chairperson

Lok Sabha

2. Shri L. K. Advani
3. Shri Prasun Banerjee
4. Dr. Sunil Baliram Gaikwad
5. Shri Hemant Tukaram Godse
6. Dr. Anupam Hazra
7. Dr. Jayakumar Jayavardhan
8. Shri P. Karunakaran
9. Shri Virendra Kashyap
10. Shri Harinder Singh Khalsa
11. Shrimati Hema Malini
12. Shri Keshav Prasad Maurya
13. Ms. Mehbooba Mufti
14. Dr. K.C. Patel
15. Shri Raosaheb Danve Patil
16. Shri Paresh Rawal
17. Dr. (Smt.) Bharatiben Dhirubhai Shiyal
18. Shri Abhishek Singh
19. Shri D.K. Suresh
20. Shri Ramdas C. Tadas
21. Shrimati R. Vanaroja

Rajya Sabha

22. Shri Javed Akhtar
23. Shri Salim Ansari
24. Shrimati Jaya Bachchan
25. Shri Vijay Jawaharlal Darda
26. Shri Meghraj Jain
27. Shri Santiuse Kujur
28. Shri Derek O'Brien
29. Dr. K.V.P. Ramachandra Rao
30. Shri Sachin Ramesh Tendulkar
31. Mahant Shambhuprasadji Tundiya

Secretariat

1. Shri K. Vijayakrishnan - Additional Secretary
2. Shri J.M. Baisakh - Director
3. Dr. Sagarika Dash - Deputy Secretary

INTRODUCTION

I, the Chairperson, Standing Committee on Information Technology (2015-2016), having been authorised by the Committee, do present the Seventeenth Report on Action Taken by the Government on the Observations/Recommendations of the Committee contained in their Fifty-second Report (Fifteenth Lok Sabha) on 'Cyber Crime, Cyber Security and Right to Privacy' of the Ministry of Communications and Information Technology (Department of Electronics and Information Technology).

2. The Fifty-second Report was presented to Lok Sabha/laid on the Table of Rajya Sabha on 12th February, 2014. The Department of Electronics and Information Technology furnished their Action Taken Notes on the Observations/Recommendations contained in the Fifty-second Report on 17th July, 2014.

3. The Report was considered and adopted by the Committee at their sitting held on 18th December, 2015.

4. For facility of reference and convenience, Observations/Recommendations of the Committee have been printed in bold in Chapter-I of the Report.

5. An analysis of Action Taken by the Government on the Observations/Recommendations contained in the Fifty-second Report of the Committee is given at Appendix-II.

New Delhi;
18 December, 2015
27 Agrahayana, 1937 (Saka)

ANURAG SINGH THAKUR,
Chairperson,
Standing Committee on
Information Technology.

CHAPTER-I

REPORT

This Report of the Standing Committee on Information Technology deals with the action taken by the Government on the Observations/ Recommendations of the Committee contained in their Fifty-second Report (Fifteenth Lok Sabha) on 'Cyber Crime, Cyber Security and Right to Privacy' relating to the Ministry of Communications and Information Technology (Department of Electronics and Information Technology).

2. The Fifty-second Report was presented to Lok Sabha/laid in Rajya Sabha on 12th February, 2014. It contained 22 Recommendations/Observations.

3. Action Taken Notes in respect of all the Observations/ Recommendations contained in the Report have been received from the Department of Electronics and Information Technology and are categorized as under:-

(i) Observations/ Recommendations which have been accepted by the Government
Rec. Sl. Nos.:- 2,3,6,7,9,11,13,14,20,21 and 22

(ii) Observations/ Recommendations which the Committee do not desire to pursue in view of the replies of the Government
Rec. Sl. Nos.:- Nil

(iii) Observations/ Recommendations in respect of which replies of the Government have not been accepted by the Committee and require reiteration
Rec. Sl. Nos.:-4, 5, and 19.

(iv) Observations/Recommendations in respect of which final replies of Government are still awaited
Rec. Sl. Nos.:- 1,8,10,12,15,16,17 and 18.

4. The Committee trust that utmost importance will be given to implementation of the Observations/Recommendations accepted by the Government. The Committee further desire that Action Taken Notes on the Observations/Recommendations contained in Chapter-I and final action taken replies to the Observations/Recommendations contained in Chapter-V of this Report should be furnished to them at an early date.

5. The Committee will now deal with action taken by the Government on some of their recommendations.

A. Challenges/Constraints relating to human resource (Auditors, Cyber Security Experts and Skill Development in IT

(Recommendation Sl. No. 4)

6. The Committee, in their original Report, had recommended as under:-

> "The Committee are given to understand that shortage of manpower is one of the major constraints in all the organisations involved in securing Indian cyber space. During the examination of Demands for Grants (2013-14), the Department had submitted that there is shortage of cyber security experts/auditors/IT skill in the country. The Committee are extremely disturbed to note that even though challenges to cyber space are on the rise, in a country with a population of around 1.21 billion, so far only around 42,000 students have been trained/undergoing training in various long-term/short-term courses and along with the existing personnel, a total of about 65,000 trained personnel are available pertaining to cyber security as against the estimated requirement of 5 lakh trained personnel. Though the Department has taken initiatives such as conducting extensive training programmes as part of the Information Security, Education and Awareness Programme (ISEA) for increasing the number of cyber security experts in the Indian Government organisations and engaging the National Security Council Secretariat with the task of determining the extent of augmentation of Cyber Security experts in the Government organizations, the Committee feel these initiatives are far from adequate. This was echoed by the Secretary, DeitY, during the course of evidence when he said 'we still have a long way to go so far as manpower in IT is concerned'.
>
> The Committee are also disappointed to note that there are only 97 Master trainers and 44 empanelled auditors by Cert-In in the country. The Department has submitted that the list of empanelled auditors has been brought down because they have to pass a stringent test. The Committee feel that while the quality and examination process cannot be compromised, the number of empanelled auditors is very less considering the requirement in the field and there is an urgent need to empanel more number of auditors to meet the requirement. The Department has also submitted that critical shortage of cyber security professionals need to be tackled in mission mode with innovative recruitment and placement procedures along with specialized training of existing manpower. The Committee, therefore, strongly recommend that the Department should make concerted efforts to increase the number of cyber security experts/auditors/IT skill in the country on top priority basis so as to ensure that shortage of manpower does not come in the way of securing Indian cyber space. The Committee may be kept apprised about the status of the increase of cyber security experts/auditors/IT skill in the country."
>
> (Para Nos. 2.8 and 2.9, Recommendation Sl. No. 4)

7. The Department of Electronics and Information Technology, in their action taken note, have stated as under:-

> "Regarding empanelment of auditors, it is submitted that the auditing organizations go through a stringent process of practical skill verification before getting empanelled under CERT-In. This empanelment process is open for all auditing organizations based in the country that possess the required skills and competency for undertaking audits and they can apply any time during a block period for empanelment. The number of organizations empanelled by CERT-In at any given point of time depends on the number of organizations that possess the required skills and qualify the practical tests.
>
> Regarding the number of cyber security experts, it is submitted that the Information Security Education and Awareness (ISEA) project of the Department has so far trained more than 42,000 persons at the formal and informal level through the involvement of around 40 institutes in the country. Continuing with this initiative, the Department has taken actions for Phase II of the ISEA Project initiation w.e.f. 1.4.2014. The project targets to train over 1,14,000 persons through various formal and informal courses with the involvement of 51 institutes."

8. Taking note of the critical shortage of cyber security professionals in the country, the Committee had recommended to the Department to increase the number of cyber security experts/auditors/personnel with IT skill on priority basis. While observing that the number of empanelled auditors is very less, the Committee had felt that there was an urgent need to empanel more number of auditors to meet the requirement. However, the Department, instead of giving any detail as to what action is being taken for increasing the number of empanelled auditors, have merely restated that auditing organizations go through a stringent process of practical skill verification before getting empanelled. The Committee feel that the Department, without compromising on the stringent procedure, should take necessary steps in imparting training and upgrading technical skill of personnel in cyber security measures so that their level of competency is enhanced, enabling more number of auditors to meet the criteria automatically and get empanelled as certified auditors.

Similarly, on the issue of increase in the number of cyber security experts, the Department have submitted that the Information Security Education and Awareness (ISEA) project being implemented by the Department have so far trained more than 42000 persons at the formal and informal level by involving around 40 institutes in the country, and that action has been taken for phase II of ISEA project targeting to train over 1,14,000 persons through various formal and informal courses by involving 51 institutes. In this regard, the

Department, however, have not clarified as to whether these formal and informal level courses train personnel to make them mere computer literate or specialize them in cyber security making them cyber security experts. In any case, considering the fact that the number of cyber security experts is very less compared to the actual requirement in the country, the Committee reiterate their earlier recommendation and urge the Department to take concrete measures to increase the pool of cyber security experts so as to tackle the growing threat of cyber security looming over the IT infrastructure of the country.

B. <u>Research and Development to secure Cyber Space</u>

(Recommendation Sl. No. 5)

9. The Committee, in their original Report, had recommended as under:-

> "The Committee note that Research and development activities are being carried out by eminent universities/organisations in areas of cyber security which *inter-alia* include (a) Cryptography and cryptanalysis, (b) Network and System Security, (c) Monitoring and Forensics and (d) vulnerability remediation and the key priority of identified areas as identified by the Department is to carry out innovative R&D with focus on basic research, technology development and demonstration, setting up test-beds, transition, diffusion and commercialization leading to widespread deployment in the field to enhance security of cyber space in the country. The Committee are, however, concerned to note that funds allocation for R&D in cyber security during the year 2012-13 could not be utilized fully due to procedural compliance for settling of pending UCs and budget for the year 2013-14 has been cut down by Rs. 10 crore (approx). This budgetary cut is a matter of extreme concern particularly when the Department has stated that large funds need to be allocated to undertake development of key technologies and present funding provided to R&D in the area of Cyber Security does not allow undertaking projects for development of strategic technologies.
>
> The Committee feel that specialised research being an important and integral part of cyber security programme, adequate attention needs to be given to this aspect with sufficient funding. The Committee, therefore, recommend that the Department should immediately take necessary steps for optimum utilisation of funds under R&D in cyber security and also facilitate research in strategic technologies. The Department should also facilitate in design of programmes for development/enhancement/promotion of skills/expertise for R&D in cyber security."

10. The Department of Electronics and Information Technology, in their action taken note, have stated as under:-

> "Cyber Security R&D programme of the Department is aimed at development / enhancement of skills and expertise in the area of cyber security by facilitating basic research in strategic technologies. Research and development is carried

out in strategic areas of cyber security including cryptography and cryptanalysis, network & system security, monitoring & cyber forensics by initiating projects in association with recognized R&D organizations. The programme has resulted in technology development as well as promotion of skills / capability development for indigenous R&D. More strategic technologies need to be developed and the Department is requesting for enhanced allocation of funds in this regard."

11. Expressing serious concern over the under-utilization of funds in R&D for cyber security during the year 2012-13 and reduction of budgetary allocations by Rs. 10 crore for the year 2013-14 owing to pending UCs, the Committee had recommended to the Department to take necessary steps for optimum utilization of funds in the R&D sector and facilitate research in strategic technologies. However, it is disquieting to note from the action taken note of the Department that no concrete steps have been taken in this direction. Apart from mentioning that R&D is being carried on in certain areas like cryptography, cryptanalysis, cyber forensics, etc., the Department have not enumerated any specific plans to facilitate research in these strategic technologies in pursuance of the recommendation of the Committee. Therefore, the Committee, while reiterating their earlier stand, once again exhort the Department to inform in clear and concrete terms about the specific steps taken for optimum utilization of fund, liquidation of pending UCs and plans for enhancement in expertise/skill in R&D for cyber security.

C. <u>Cyber Appellate Tribunal (earlier known as Cyber Regulations Appellate Tribunal)</u>

(Recommendations Sl. No. 19)

12. The Committee had recommended as under:-

"The Committee note that the Cyber Regulations Appellate Tribunal (CRAT) was established in October, 2006 in accordance with the provision contained under Section 48(1) of the IT Act 2000, and after the amendment of the IT Act in the year 2009, the Tribunal is known as Cyber Appellate Tribunal (CAT). As per the IT Act, any person aggrieved by an order made by the Controller of Certifying Authorities or by an Adjudicating Officer under the Act can appeal before the Cyber Appellate Tribunal (CAT). The main objectives of the Cyber Appellate Tribunal is to consider and decide the validity/legal propriety of the orders passed by the Adjudicating Officers and to spread awareness about the Cyber Appellate Tribunal (CAT) mechanism for redressing the grievances of the aggrieved party against the orders of the Adjudicating officers appointed under IT Act 2000 and 2008. The Committee also note that till date there is only one Cyber Appellate

Tribunal in the country though the Act provides for setting up Benches in other parts of the country which has not yet been done. The Committee are surprised to learn that since inception of CAT only 17 appeals have been disposed off by the former Chairperson and 21 appeals are still pending for hearing in the Tribunal which are scheduled for disposal on appointment of the new Chairperson. The Committee are also given to understand that Member (Technical) has taken over the charge in the month of December 2012 and CAT is making efforts to discharge their responsibilities with the existing manpower and steps have been initiated to recruit additional manpower for its effective functioning. While expressing their displeasure over the undue delay taking place in disposal of appeal by the Cyber Appellate Tribunal, the Committee strongly recommend the Department to deploy adequate manpower at the earliest so that appeals that are pending for hearing in the Tribunal are disposed of expeditiously. Efforts may also be made to set up CAT branches in other parts of the country, if need arises. The Committee may be kept apprised about the disposal status of cases before CAT."

(Para No. 2.26, Recommendation Sl. No. 19)

13. The Department of Electronics and Information Technology, in their action taken note, have stated that they have taken steps for appointment of Chairperson for the Cyber Appellate Tribunal and Rule No. 13 of the Cyber Regulation Appellate Tribunal (Procedure) Rules, 2000 provides for hearing the appeal at any place of the country to cater to the needs of other parts of the country. Further, Video conferencing facility has been established in 24 States and UTs to enable litigation of the remote areas to plea their cases remotely.

14. While observing that there is only one Cyber Appellate Tribunal (CAT) in the country and in view of the pendency of cases in the Tribunal, the Committee had recommended to the Department to deploy adequate manpower at the earliest so that the pendency of appeals could be disposed off expeditiously by the Tribunal. The Committee had also recommended to the Department to make efforts for setting up CAT Benches in other parts of the country. In this regard, though the Department have informed that they have taken steps for appointment of Chairperson or the CAT, the action taken reply does not indicate any timeline as to by what time the Chairperson will be appointed. The Department have also not addressed that part of the recommendation wherein the Committee had specifically recommended to deploy adequate manpower and wanting to know the actual status of disposal of cases before CAT. While expressing their displeasure over the way the issue has been dealt with, the Committee reiterate their earlier recommendation and call upon the Department to expedite the appointment of the Chairperson for CAT within a specified timeframe and also deploy adequate manpower in CAT so that the appeals pending in the Tribunal are disposed off expeditiously and the Committee be apprised of the disposal status

of all the 21 appeals pending. The Committee may also be apprised as to how video conferencing facility established in the 24 States and UTs has facilitated the remote appeal process and helped in quick disposal of cases relating to cyber crime.

CHAPTER-II

OBSERVATIONS/RECOMMENDATIONS WHICH HAVE BEEN ACCEPTED BY THE GOVERNMENT

Cyber-Crime and Financial Losses

(Recommendations Sl. No. 2)

The Committee are concerned to note that there has been a consistent increase in cyber crime cases in the country during last five years. As per the cyber-crime data maintained by National Crime Records Bureau (NCRB), a total of 420, 966, 1791 and 2876 Cyber Crime cases were registered under Information Technology Act during the years 2009, 2010, 2011 and 2012 respectively, and a total of 276, 356, 422 and 601 cases were registered under Cyber Crime related Sections of Indian Penal Code (IPC) during 2009, 2010, 2011 and 2012 respectively. In addition, number of Cyber Crime cases registered by Central Bureau of Investigation (CBI) during the years 2010, 2011 and 2012 under provisions of Information Technology Act 2000 and other acts were 10, 12 and 11 respectively. The Committee find it disquieting to note that the quantum of financial loss and privacy related cases in the country due to cyber-attack/fraud in last few years have increased. According to the Reserve Bank of India (RBI), in the last five years though the number of fraud cases reported by Banks on account of ATM Debit Cards/Credit Cards/Internet have decreased from 15018 (in 2010) to 8322 (in 2012), yet the amount involved had increased from Rs. 40.48 crore in 2010 to Rs. 52.67 crore in 2012. Further, the number of cases registered by CBI pertaining to financial frauds under the provisions of Information Technology Act 2000 ranged between 6 to 8 during 2008 to 2011 and amount involved increased from Rs. 6.42 crore to Rs. 28.79 crore. The Committee are of the view that the reported number of cases involving financial fraud due to cyber related cases is just tip of the iceberg as a number of cases go unnoticed and unreported.

The Committee are unhappy to note that as of now there are several agencies which are involved in maintaining separate data with regard to cyber crime cases. National Crime Records Bureau (NCRB) under Ministry of Home Affairs (MHA) is maintaining data on cyber frauds. The mechanism for recording data with regard to Internet financial frauds, along with quantum of loss, is being maintained by Reserve Bank of India and Central Bureau of Investigation (CBI). The Committee have been informed that DeitY regularly interacts with Banks, RBI and CBI regarding cyber frauds related actions such as prevention, investigation, support, technical advisories, promotion of best practices and compliances, yet in view of ever increasing incidence of cyber crime cases and their impact on country's security, finance and economy as a whole the Committee fail to understand as to how the Department concretises its cyber security strategies when so many agencies are involved in data collection and maintenance and when there is absence of any centralised monitoring system and centralised maintenance of data relating cyber fraud. The Committee feel that there should be one single, centralised cell/agency to deal with all cases of cyber crime/threat in the country. This will not only help the Department in knowing the pattern of the crime but also prevent recurrence of same kind of crimes with newer strategies. The Committee, therefore, recommend the Department to work in the above direction and apprise the Committee of the action taken in this regard.

Reply of the Government

Issues related to cyber crime are under the business domain of Min. of Home Affairs (MHA). Further, Law and Order being a state subject, all actions related to crime including cyber crime are dealt with by respective states/UTs. Many of the states have set up cyber crime cells which are monitoring such crimes. At the national level, relevant data is being maintained by single agency i.e. National Crime Records Bureau (NCRB) under MHA. DeitY is closely working with MHA and other agencies.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

Challenges/Constraints relating to human resource (Auditors, Cyber Security Experts and skill development in IT)

(Recommendations Sl. No. 3)

The Committee note that the complex inter-connectivity of Internet with borderless environment, evolving innovative technologies, lack of awareness and rapidly changing security and threat landscape has posed massive challenge to cyber security ranging from data theft, espionage and Denial of Service (DoS) attacks to offensive actions by adversarial State and Non-State actors. The Committee also note that anonymous attacks – groups sponsored by Nations and terrorist groups also have become a major cross border challenge in Cyber Space.

The Committee are unhappy to note that though all critical sector organizations under Central Government Ministries/Departments are mandated to implement information security best practices as per ISO 27001, there are 546 organizations in the country which have obtained the ISO 27001 certification. What is more intriguing is that the Department has not made any effort to ascertain as to why all the Government organisations have failed to obtain ISO 27001 certification. The Committee need not emphasise that adhering to information security best practices helps in containing the cyber crime to a great extent. Therefore, the Committee recommend the Department to take necessary steps in identifying the reasons for all the Government Departments/ organisations for not following the information security best practices and urge upon them to expeditiously obtain ISO 27001 certification to enable them to adhere to information security best practices.

Reply of the Government

The approach to implementing security best practices in Govt. and critical sector organizations is taken up by way of implementing a comprehensive Cyber Crime Management Plan (CMP) for Countering Cyber Attacks and Cyber Terrorism. The CMP has been approved by the National Crisis Management Committee for wider circulation and implementation among key central Ministries, all States & UTs and critical sector organizations within their domain. The implementation of Cyber Crisis Management Plan along with implementation of security best practices is being regularly reviewed by the Department as well as Secretary, Security in the Cabinet Secretariat for periodic reporting to the National Crisis Management Committee. The Ministries/ Departments have taken several steps and implementation of CMP is well in progress. In order to assist the organizations for implementing the CMP as well as security best

practices, the Department is providing assistance in form of guidelines, templates and self-assessment tools besides conducting enabling workshops. Secretary, Security is making specific efforts in urging the organizations for implementing Crisis Management Plan and security best practices on priority.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

Cyber Crime Cell and Cyber Crime Lab

(Recommendation Sl. No.6)

The Committee note that there is Cyber Forensics training lab at Training Academy of Central Bureau of Investigation (CBI) to impart basic and advanced training in cyber forensics and investigation of cyber-crimes to Police Officers associated with CBI. The Committee also note that the Government has also set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States. The Committee are of the strong opinion that there is an urgent need to increase the number of cyber-crime cells and labs in the States and provide requisite manpower, training and infrastructure to them. The Committee, therefore, recommend the Department to take concrete initiatives in setting up the cyber-crime cells and labs in States where these do not exist and also upgrade and strengthen the existing cyber crime cells with adequate fund and infrastructure so as to cope up with the rapid cyber threat and privacy infringement.

Reply of the Government

Department has set up Cyber Crime investigation training Labs for Law Enforcement and judiciary in CBI, Kerala and all the states of Northeast to facilitate training to the Police and judicial officers with regard to Cyber crime forensic and legal aspects. In addition, Cyber Forensics Training Labs for Police have been setup at Pune, Kolkata, Bangalore and Mumbai. Awareness Workshops are being organised regularly in major cities to sensitize the police officers. MHA, under the cyber crime investigation program, is supporting establishment of Cyber Crime Police Station (CCPS) and Cyber Crime Investigations and Forensic Training Facilities (CCIFTF) in each state/UT of India under police modernization scheme. The Department is working with High Courts in the country to train judicial officers in the area of cyber crimes and interpreting electronic evidence.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

Budgetary allocations to tackle the Cyber threats

(Recommendations Sl. No. 7)

The Committee note that even though the expenditure pattern has been Rs. 20-30 crore on an average for each year for tackling cyber threat, a sum of Rs. 500 crore has been allocated for Twelfth Five Year Plan against the proposed sum of Rs. 1500 crore. The Secretary, DeitY,

informed the Committee that the Department proposes to approach the Planning Commission for allocation of more funds. However, considering the quantum increase in allocation and keeping in view the continuous under-utilisation of funds, the Committee trust that with higher allocations received for the current Plan period as compared to earlier years the Department will increase their capacity building for carrying the programmes so as to utilise the allocated funds and achieve the desired objectives.

Reply of the Government

In support of the National Cyber Security Policy objectives, the Department has taken steps to initiate key projects in the area of cyber security commensurating with the allocation made for the program during the 12th Plan. Allocation of more funds is needed.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

Concerns associated with upcoming technology

(Recommendations Sl. No. 9)

The Committee observe that National e-Governance Programme (NeGP) is one of the ambitious projects of the Government and the Department is planning to use 'Cloud computing' for e-Governance Programmes and for storing its data. The Committee also note that the Government of India has recently published GI Cloud (Meghraj) – 'Strategic Direction Paper' and 'Adoption and implementation Roadmap' as a part of this Cloud initiative which prescribes the precautions, standards and guidelines on security addressing the various challenges and risks and gives more clear dimension to the timelines of implementation. With regard to the usage of 'Cloud computing', the Committee in their Twenty-seventh Report (2011-12), had expressed apprehensions about technological and legal challenges associated with the concept of 'shared platform' and had recommended the Department to conduct a study/survey to find out the existing scenario nationally and internationally and be prepared with a mechanism to deal with the risks associated with the usage of Cloud computing and be vigilant about such emerging technologies. However, the Committee are surprised to note that though NeGP has entered seventh year of its implementation, the Department has neither conducted any study/survey in this regard nor has any data on instances of cyber security breaches encountered in e-Governance projects. The Committee feel that NeGP being a visionary project of the Government, the Department should not show any laxity. The Committee, therefore, recommend the Department to conduct a study/survey to find out the instances of cyber security breaches in NeGP projects. While cautioning the Department to be extra vigilant with the usage of the new technology 'cloud' which is still at a nascent stage, the Committee desire that the Department would stick to their assurance of keeping security issues on priority, particularly, in the implementation of e-Governance projects and make the programme foolproof.

Reply of the Government

As per the two (2) policy papers published by the Department in June, 2013, the National Clouds are being established in India for providing cloud service to government departments / ministries . The IT services over cloud are hosted in India. The first National cloud is implemented by NIC which is owned and managed by Government. As part of SDC phase-II, every State Data Centre is being upgraded for providing cloud services to the line departments in their respective State. The Department is also in the process of setting up Cloud Management Office (CMO), which will be responsible for coming up with the necessary policies and guidelines on interoperability, integration, data security, portability, operational aspects, contract management, etc. which will help us in addressing security and risk challenges.

The Department has conducted a study tour to three pilot states to understand the security posture of e-Gov Infrastructure. Based on the study, an advisory was issued by Department to all the states to plug the shortcomings.

To assure security in e-Gov projects and prevent security breaches, the Department has developed an e-Governance security policy document for guiding the top management and implementation level guidelines for operational level personnel involved in implementing e-Gov projects at state and central level.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

MoUs and International Treaties

(Recommendations Sl. No. 11)

The Committee note that in a globalised economy, a focused approach to international relations is vital particularly in case of cyber-space which by its very nature is borderless and anonymous. The Committee also note that the Department has taken numerous collaborative efforts and has geared up to encourage sustainable development and strengthening partnerships with other countries. In addition, 'National Cyber Security Policy (NCSP)-2013' provides for information sharing and cooperation arrangements with other countries to develop bilateral and multi-lateral relationships in the area of cyber security with other countries and to enhance national and global cooperation among security agencies, CERTs, Defence agencies and forces, Law Enforcement agencies and the judicial systems. The Committee are also given to understand that Department enters into international cyber security cooperation arrangements with organizations engaged in similar activities, in the form of Memorandum of Understandings (MoUs) and in case of absence of MoUs with some countries, the provisions of MLAT (Mutual Legal Assistance Treaty) are used for eliciting support for cyber crime cases. The Committee are happy to note that the Department has signed MoUs in the area of cyber security with USA, Japan, South Korea, Mauritius, Kazakhstan, and Finland and during the year 2012-13, MoU has also been signed with Canada in ICT and Electronics sector. Further, the Department with active assistance of the Ministry of External Affairs, is also having engagement dialogue with several countries such as Malaysia, Israel, Egypt, Canada,

Brazil that are willing to cooperate and share information with regard to cyber security incidents and vulnerabilities in IT products and systems. While appreciating the above initiatives, the Committee desire the Department to continue with these initiatives and enter into MOUs and exchange programmes with more number of countries for having legal and technical tie-ups for addressing the cross border challenges associated with cyber security.

Reply of the Government

The Department with the active assistance of Ministry of External Affairs (MEA) is having engagement / dialogues with various countries that are willing to cooperate and share information with regard to cyber security incidents and vulnerabilities in IT products and systems.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

Preparedness/Policies/legal Initiatives to address the issue (IT Act and Cyber Security)

(Recommendation Sl. No. 13)

The Committee note that keeping in view the security risks and vulnerabilities of the internet/computer run systems like defence establishments, hospitals, transportation, Banks, Government organisations, Government has taken several steps to improve the alertness of the Government and other critical sector organisations and as part of Cyber Crisis Management Plan (CCMP) for countering cyber attacks and cyber terrorism , all Ministries/Departments of Centre/State Governments and their organisations and critical sectors have been mandated to continuously assess the posture of their IT systems and networks. In addition, the Department has advised organizations to report the cyber security incidents to CERT-In within one hour of occurrence of the cyber attack incident or noticing the incident. The Committee recommend that CCMP should be frequently reviewed and revised so as to keep pace with the rapid changing nature of cyber threats. Further, DeitY should ensure that all the Central Ministries/Departments/ Organisations/State Governments implement the Cyber Crisis Management Plan (CCMP) in right earnest.

Reply of the Government

The cyber Crisis Management Plan is being reviewed and revised on periodic basis every year and reflects the changing nature of cyber threats and related response measures. The implementation of Cyber Crisis Management Plan along with implementation of security best practices is being regularly reviewed by the Department as well as Secretary, Security in the Cabinet Secretariat for periodic reporting to the National Crisis Management Committee. In order to assist the organizations for implementing the CMP as well as security best practices, the Department is providing assistance in the form of guidelines, templates and self-assessment tools besides conducting enabling workshops. Secretary, Security is making specific efforts in urging the organizations for implementing Crisis Management Plan and security best practices on priority.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

(Recommendation Sl. No. 14)

The Committee have also been informed that there are provisions under Sections 43 A, 66 A, 67, 69 B, 70 (1), 70 (4), 70-B, 72 A, 79 and 84 A, in the Information Technology Act, 2000 (IT Act) to address to the problems relating to cyber crime. On the issue of adequacy of the existing legal frame work for dealing with the cyber-crimes, the Department has stated that IT Act, 2000 addresses all aspects related to cyber crimes in a comprehensive manner with adequate compliance and deterrent provisions and at present, there is no need to amend the Information Technology Act to address National Cyber Security Policy. At the same time, the Department has also stated that since it is a dynamic area, the IT Act will be amended as and when needed. The Committee are of the view that even though the existing provisions of IT Act, 2000 may seem adequate to address all aspects related to cyber crimes in a comprehensive manner in the present circumstances, in view of the recent uproars over Section 66A of IT Act and in the light of everyday development in the area, the Department needs to put in place a system of periodical review of the existing provisions in various Sections of the Act. The Committee, therefore, urge the Department to take the above issue seriously so as to have preparedness on all provisions as the entire country is rapidly becoming dependent on Information Technology.

Reply of the Government

As provided in Section 88(1) of the Information Technology Act 2000, a Cyber Regulation Advisory Committee (CRAC) has been constituted to advise the Central Govt. either generally as regards any rules or for any other purpose connected with the Act.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

<u>Education/Awareness/Training</u>

(Recommendation Sl. No. 20)

The Committee appreciate that the Ministry of Home Affairs has advised State Governments and Union Territory Administrations to build adequate technical capacity in handling cyber crime including technical infrastructure, cyber police stations and trained manpower for detection, registration, investigation and prosecution of cyber crimes. The Committee also note that the Government has formulated a set of investigation manuals with procedures for Search, Seizure Analysis and Presentation of digital evidence in courts. The manuals have been circulated to Law Enforcement Agencies in all States. In view of technical expertise required in handling cyber crime, the Committee are of the opinion that mere issuance of advisories would not solve the problem. Rather, the Department should proactively coordinate with the Ministry of Home Affairs/State Governments for building up the capacity/training police personnel for detection, registration, investigation, handling of cyber crime evidences, etc.

Reply of the Government

Department has set up Cyber Crime investigation training Labs for Law Enforcement and judiciary in CBI, Kerala and all the states of Northeast to facilitate training to the Police and judicial officers with regard to Cyber crime forensic and legal aspects. In addition, Cyber Forensics Training Labs for Police have been setup at Pune, Kolkata, Bangalore and Mumbai.

Awareness Workshops are being organised regularly in major cities to sensitize the police officers. MHA, under the cyber crime investigation program, is supporting establishment of Cyber Crime Police Station (CCPS) and Cyber Crime Investigations and Forensic Training Facilities (CCIFTF) in each state/UT of India under police modernization scheme..

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

(Recommendation Sl. No. 21)

The Committee further note that in order to gauge the level of cyber security preparedness as well as awareness in the country, the Department has initiated a project 'National e-Security Index' in association with Data Security Council of India (DSCI) and the project is expected to enable studies and surveys in different sectors and segments in the country and provide information in the form of an index that can guide policy related actions in the country. The Committee recommend that the project should be implemented expeditiously and the Committee may be apprised of its status/outcome.

Reply of the Government

Developmental efforts for creation of model for depiction of National e-Security Index is complete and the same has been validated using test data.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

(Recommendation Sl. No. 22)

The Committee are extremely unhappy to note that when asked about the initiatives taken by the Government to create awareness about cyber-crime amongst children, the Department has furnished exactly the same reply that was provided to the Committee during the examination of Demands for Grants (2011-12) which *inter-alia* include 150 workshops organised in schools covering 20,000 students upto 10^{th} Grade. In view of the non-availability of updated information, the Committee are unable to assess the action taken by the Department after 2011 and are not sure whether awareness/workshops have been conducted by the Department thereafter. The Committee would like the Government to take up projects/schemes for awareness programmes for children on continuous basis. The Department should also take necessary action in coordination with concerned authorities to make the curriculum of cyber security mandatory in schools syllabus. In addition to this, the Committee also recommend the Department to set up a national help line/call centre for common public which can guide them about dealing with cyber crime and redressal mechanism. The Committee may be apprised about the Department's concrete action in this regard.

Reply of the Government

Department has implemented Information Security Education and Awareness (ISEA) project w.e.f. March 2005 onwards. Awareness workshops for school children, college students etc. are designed and conducted. These workshops are conducted at various locations through

the centres of C-DAC, NIELIT and other participating institutes of ISEA project. So far 623 workshops have been organized across the country covering about 21,600 Teachers / Parents / CSC / NGOs, including various Government officers etc., and about 60,100 school children / Engg. or Degree college students. During these workshops, around 50,500 Awareness Kits (with promotional material, Booklets and Hand Books) were distributed. Further, around 50 posters on various topics of Information Security Awareness have been designed and around 1,20,000 posters were distributed to target users in schools, colleges, etc.

A dedicated website for information security awareness (http://www.infosecawareness.in) has been developed and launched by C-DAC, Hyderabad. The website includes separate sections for Children, Students and Parents where various aspects on guidelines, security risks and tips, understanding of security concepts etc. have been included. Further, around Forty (40) cartoon/ animation (3D/2D) videos have been developed and made available through this websites for downloads. Course material like guidelines for XP, Windows server 2008, Vista, Linux, wireless configurations developed. Several security e-Books have been developed (Security Guidebook, Security Tool Kit, Children Hand Book, Guidebook for Teachers and Parents) and made available on the web site. There are around 9800 downloads so far. Hindi, Malayalam, Kannada versions of Security Awareness Handbook has been developed.

Twelve (12) e-newsletters were designed and distributed through email / website. 12 newsletters were designed, printed and distributed across 10,000 colleges, schools and government organizations. Information Security Awareness Diary for 2009, 2011, 2012, 2013 with 365 tips; 365 Days Information Security tips calendar; Wall calendar for 2011, 2012, and 2013; Table top calendar for the year 2010 and 2012; Pocket Calendar for 2012 were designed and developed.

To sensitize and create awareness about safe use of Electronic devices among citizens, Multimedia based Multi-lingual brochures highlighting secure use of devices designed and being distributed along with the devices by the manufacturers. A website has also been hosted to promote awareness for securing devices.

A project is on-going in Northeast in the states of Mizoram, Nagaland and Tripura to create awareness among school and college students. Awareness programmes are regularly conducted in schools and colleges identified by the State Government in these states.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

CHAPTER –III

OBSERVATIONS/RECOMMENDATIONS WHICH THE COMMITTEE DO NOT DESIRE TO PURSUE IN VIEW OF THE REPLIES OF THE GOVERNMENT

--NIL--

CHAPTER –IV

OBSERVATIONS/RECOMMENDATIONS IN RESPECT OF WHICH REPLIES OF THE GOVERNMENT HAVE NOT BEEN ACCEPTED BY THE COMMITTEE AND WHICH REQUIRE REITERATION

Challenges/Constraints relating to human resource (Auditors, Cyber Security Experts and skill development in IT)

(Recommendations Sl. No. 4)

The Committee are given to understand that shortage of manpower is one of the major constraints in all the organisations involved in securing Indian cyber space. During the examination of Demands for Grants (2013-14), the Department had submitted that there is shortage of cyber security experts/auditors/IT skill in the country. The Committee are extremely disturbed to note that even though challenges to cyber space are on the rise, in a country with a population of around 1.21 billion, so far only around 42,000 students have been trained/undergoing training in various long-term/short-term courses and along with the existing personnel, a total of about 65,000 trained personnel are available pertaining to cyber security as against the estimated requirement of 5 lakh trained personnel. Though the Department has taken initiatives such as conducting extensive training programmes as part of the Information Security, Education and Awareness Programme (ISEA) for increasing the number of cyber security experts in the Indian Government organisations and engaging the National Security Council Secretariat with the task of determining the extent of augmentation of Cyber Security experts in the Government organizations, the Committee feel these initiatives are far from adequate. This was echoed by the Secretary, DeitY, during the course of evidence when he said 'we still have a long way to go so far as manpower in IT is concerned'.

The Committee are also disappointed to note that there are only 97 Master trainers and 44 empanelled auditors by Cert-In in the country. The Department has submitted that the list of empanelled auditors has been brought down because they have to pass a stringent test. The Committee feel that while the quality and examination process cannot be compromised, the number of empanelled auditors is very less considering the requirement in the field and there is an urgent need to empanel more number of auditors to meet the requirement. The Department has also submitted that critical shortage of cyber security professionals need to be tackled in mission mode with innovative recruitment and placement procedures along with specialized training of existing manpower. The Committee, therefore, strongly recommend that the Department should make concerted efforts to increase the number of cyber security experts/auditors/IT skill in the country on top priority basis so as to ensure that shortage of man power does not come in the way of securing Indian cyber space. The Committee may be kept apprised about the status of the increase of cyber security experts/auditors/IT skill in the country.

Reply of the Government:

Regarding empanelment of auditors, it is submitted that the auditing organizations go through astringent process of practical skill verification before getting empanelled under CERT-In. This empanelment process is open for all auditing organizations based in the country that possess the required skills and competency for undertaking audits and they can apply any time

during a block period for empanelment. The number of organizations empanelled by CERT-In at any given point of time depends on the number of organizations that possess the required skills and qualify the practical tests.

Regarding the number of cyber security experts, it is submitted that the Information Security Education And Awareness (ISEA) project of the Department has so far trained more than 42,000 persons at the formal and informal level through the involvement of around 40 institutes in the country. Continuing with this initiative, the Department has taken actions for Phase II of the ISEA Project initiation w.e.f. 1.4.2014. The project targets to train over 1,14,000 persons through various formal and informal courses with the involvement of 51 institutes.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

Comments of the Committee
(Please see Para No. 8 of Chapter I)

Research and Development to secure Cyber Space

(Recommendation Sl. No. 5)

The Committee note that Research and development activities are being carried out by eminent universities/organisations in areas of cyber security which *inter-alia* include (a) Cryptography and cryptanalysis, (b) Network and System Security, (c) Monitoring and Forensics and (d) vulnerability remediation and the key priority of identified areas as identified by the Department is to carry out innovative R&D with focus on basic research, technology development and demonstration, setting up test-beds, transition, diffusion and commercialization leading to widespread deployment in the field to enhance security of cyber space in the country. The Committee are, however, concerned to note that funds allocation for R&D in cyber security during the year 2012-13 could not be utilized fully due to procedural compliance for settling of pending UCs and budget for the year 2013-14 has been cut down by Rs. 10 crore (approx). This budgetary cut is a matter of extreme concern particularly when the Department has stated that large funds need to be allocated to undertake development of key technologies and present funding provided to R&D in the area of Cyber Security does not allow undertaking projects for development of strategic technologies. The Committee feel that specialised research being an important and integral part of cyber security programme, adequate attention needs to be given to this aspect with sufficient funding. The Committee, therefore, recommend that the Department should immediately take necessary steps for optimum utilisation of funds under R&D in cyber security and also facilitate research in strategic technologies. The Department should also facilitate in design of programmes for development/enhancement/promotion of skills/expertise for R&D in cyber security.

Reply of the Government

Cyber Security R&D programme of the Department is aimed at development / enhancement of skills and expertise in the area of cyber security by facilitating basic research in strategic technologies. Research and development is carried out in strategic areas of cyber security including cryptography and cryptanalysis, network & system security, monitoring &

cyber forensics by initiating projects in association with recognized R&D organizations. The programme has resulted in technology development as well as promotion of skills / capability development for indigenous R&D. More strategic technologies need to be developed and the Department is requesting for enhanced allocation of funds in this regard.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

Comments of the Committee
(Please see Para No. 11 of Chapter I)

Cyber Appellate Tribunal (earlier known as Cyber Regulations Appellate Tribunal)

(Recommendation Sl. No. 19)

The Committee note that the Cyber Regulations Appellate Tribunal (CRAT) was established in October, 2006 in accordance with the provision contained under Section 48(1) of the IT Act 2000, and after the amendment of the IT Act in the year 2009, the Tribunal is known as Cyber Appellate Tribunal (CAT). As per the IT Act, any person aggrieved by an order made by the Controller of Certifying Authorities or by an Adjudicating Officer under the Act can appeal before the Cyber Appellate Tribunal (CAT). The main objectives of the Cyber Appellate Tribunal is to consider and decide the validity/legal propriety of the orders passed by the Adjudicating Officers and to spread awareness about the Cyber Appellate Tribunal (CAT) mechanism for redressing the grievances of the aggrieved party against the orders of the Adjudicating officers appointed under IT Act 2000 and 2008. The Committee also note that till date there is only one Cyber Appellate Tribunal in the country though the Act provides for setting up Benches in other parts of the country which has not yet been done. The Committee are surprised to learn that since inception of CAT only 17 appeals have been disposed off by the former Chairperson and 21 appeals are still pending for hearing in the Tribunal which are scheduled for disposal on appointment of the new Chairperson. The Committee are also given to understand that Member (Technical) has taken over the charge in the month of December 2012 and CAT is making efforts to discharge their responsibilities with the existing manpower and steps have been initiated to recruit additional manpower for its effective functioning. While expressing their displeasure over the undue delay taking place in disposal of appeal by the Cyber Appellate Tribunal, the Committee strongly recommend the Department to deploy adequate manpower at the earliest so that appeals that are pending for hearing in the Tribunal are disposed of expeditiously. Efforts may also be made to set up CAT branches in other parts of the country, if need arises. The Committee may be kept apprised about the disposal status of cases before CAT.

Reply of the Government

Department has taken steps for appointment of Chair-person for the Cyber Appellate Tribunal. Rule No. 13 of the Cyber Regulation Appellate Tribunal (Procedure) Rules 2000 provides for hearing the appeal at any place of the country to cater to the needs of other parts of the country. Further, Video conferencing facility has been established in 24 states and UTs to enable litigation of the remote area to plea their cases remotely.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

Comments of the Committee
(Please see Para No. 14 of Chapter I)

CHAPTER –V

OBSERVATIONS/RECOMMENDATIONS IN RESPECT OF WHICH REPLIES ARE OF INTERIM IN NATURE

Increase in Cyber-Crime Cases and Preparedness to tackle the issue

(Recommendations Sl. No. 1)

The Committee note that Indian cyber landscape has seen a significant increase in spam and phishing activities, virus and warm infections, Bot Net infected systems, etc. and were apprised of 20 types of cyber crime being witnessed worldwide. The Committee are sure by the time this Report is tabled many more computer viruses/malwares may have been reported/noticed making our systems more vulnerable and prone to attacks.

The Committee are concerned to note that the number of incidents of website compromise in India has grown 5.5 times during the last 5 years (2007-08 to 2013-14) making the country amongst top five countries with respect to spam mail. Further, the phishing incidents have increased from 392 to 887 during the same period. Resultantly cyber crime threat incidents handled by the Cert-In have also increased considerably during this period. Further, 20 different categories of threats have been identified against which whole cyber space is required to be protected. The Secretary, DeitY, during the course of evidence was candid in admitting that the nature and size of the threat in cyber space in India is looming large and it is very much important to protect eleven critical sectors such as power, atomic energy, space, aviation, transportation, etc. which are predominantly using IT systems. The Committee feel that in a rapidly changing scenario where all the systems are getting integrated rapidly through IT infrastructure and upcoming technologies such as cloud, it is imperative that our preparedness to face challenges emanating from any kind of cyber attack is hundred per cent full proof. Therefore, the Committee recommend that the Department should put the proposed agenda of 24x7 National Critical Information Infrastructure protection centre, which aims to protect the critical information infrastructure in the country, on top priority and implement its cyber security programmes expeditiously so that any kind of cyber attack have no impact on functioning of our critical sectors.

Reply of the Government

In respect of National Critical Information Infrastructure Protection Centre (NCIIPC), Govt. has notified the following:

i) Designating the National Critical Information Infrastructure Protection Centre, an organization under National Technical Research Organization (NTRO), as a national nodal agency in respect of critical information infrastructure protection.

ii) Information Technology (National Critical Information Infrastructure Protection Centre and manner of performing functions and duties) Rule, 2013.

The National Critical Information Infrastructure Protection Centre is in the process of identifying the critical centers and related information infrastructure for notification under Section 70 of Information Technology Act 2000.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

Threat from imported electronics/IT products and hosting of servers outside India (Need for Certification unit and hosting of servers in India)

(Recommendations Sl. No. 8)

The import of electronic/IT products and hosting of servers outside India pose major threat to the country's security in general and threat to the citizen's security and privacy in particular. The Committee in their Thirty-fourth Report on Demands for Grants (2012-13) had raised their concern over the risks involved with imported electronics/IT products and recommended the Department to take action in this regard. The Committee are, however, unhappy to note that the country depends largely on imported electronics and majority of the websites are still being hosted outside India. The Committee are given to understand that hosting of websites/servers outside India is largely on account of economical and cost advantage reasons because the protection mechanism for securing websites involves significant expenditure. The Department itself has admitted that there are Technical concerns *viz*. attack attribution for counter action and Legal concerns *viz*. cooperation and jurisdictional issues due to location of internet servers outside country. The Committee also note that the Government has adopted strategies to deal with the hassles which include issuance of advisories to all intermediaries including national and international service providers, regular dialogue with the intermediaries, notification of a 'Framework and Guidelines' for use of Social Media by its agencies, etc. In addition, the Department has drafted a 'e-mail policy' and 'data storage policy' for the Central Government and the State Governments which would not only mandate all Government employees to use the Government mail services, but would also prohibit usage of private services hosted whether in India or abroad (as the confidential and nationally sensitive data etc. in 99 percent of the cases emanate from the Government organisations). While all these initiatives have been taken note of, keeping in view the security aspects the Committee emphasize that the Government should take measures, as far as possible, to locate internet servers for critical sectors within the country.

The Committee note that under the Common Criteria Project of DeitY, STQC has established the Indian Common Criteria Certification Scheme (IC3S) at STQC, New Delhi and a full-fledged laboratory at Kolkata, with a capability for testing and certification of security of IT Products as per International standards, ISO/IEC 15408, based on Common Criteria Standards up to EAL4. Presently, evaluations are undertaken for certification of IT products like operating systems of routers, switches and firewalls; security appliances upto EAL4. The Committee are happy to note that India has become 17th 'Authorizing Nation' under Common Criteria Recognition Arrangement (CCRA) and that henceforth the product tested and certified under

Common Criteria Certification Scheme up to Assurance Level 4 (EAL4) are acceptable not only in India but also in other member countries of CCRA without re-testing under the mutual recognition arrangements. It is also noted that the present scope of certification is limited to network boundary protection device and general purpose operating systems and STQC does not have necessary expertise and knowledge in highly complex products such as Radar etc. The Committee have been informed that in view of increasing penetration of ICT in the country, STQC Directorate has initiated steps to enhance its capacity for testifying IT products as part of its action in Twelfth Plan. In addition, the sub group on testing and certification infrastructure under the Joint Working Group for public Private Partnership on Cyber Security also envisage setting up of such testing Infrastructure with active participation from private sector. The Committee desire that all efforts should be made with due promptitude to create the infrastructure and to enhance the capacity of STQC for testing of IT products. The Committee also recommend the Department to host more and more servers in India. Not only this, the Department should also have stringent measures to safeguard the indigenous servers as most of the cyber attacks are in '.in' domain. In addition, the Department should lay down provisions for mandatory certification for all imported electronics/IT/telecom products and have certification centres in each State/UT specifically at all the airports/naval docks/ international borders.

Reply of the Government

Government has issued guidelines to host the websites of Govt, Ministries/Department and other Govt. services on servers located with secure infrastructure service providers in India. It has been mandated that all new Govt websites and applications are to be audited with respect to cyber security prior to their hosting. National Informatics Center (NIC) hosts the Govt. websites and the hosted sites are located in National data centres established within the country. NIC facilitates the Government departments to host their sites on NICNET data centres. NIC has taken various security measures including auditing of sites, deployment of Firewalls, Intrusion Prevention Systems, Antivirus solutions and 24x7 monitoring. NIC has accorded security issues high priority and has put in place due diligence mechanisms & controls encompassing all aspects of people, process & technology.

Further, both the primary and the secondary DNS servers in respect of .IN Registry are hosted within the country. Further, to safeguard the indigenous .IN servers, .IN Registry has put in place the following measures:

- Access to .IN domains is performed via a highly redundant, global, Anycast DNS network, which protects against massive distributed denial of service (DDOS) attacks.
- .IN registry is secured behind a 5 layer security ring with all critical components fully redundant hardware software and service provision including a completely functional and tested disaster recovery facility.

Department of Electronics and Information Technology has framed E-mail policy. The said policy has been discussed with concerned Ministries & Departments. The Committee of Secretaries have also deliberated on this policy. The Policy envisages e-mail servers to be located in India.

STQC Directorate of the Department established Common Criteria Test Lab at ERTL Kolkata. In order to enhance the capacity for security testing and evaluation of IT products in

the country, STQC has initiated steps to draft guidelines and procedures for empanelment of Common Criteria Test Labs in public and private sectors.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

Co-operation/coordination with other organizations/countries (NCIIPC, all Ministries, Departments, Cyber Appellate Tribunal, CERT-In, Police) PPP and efficacy of organizations

(Recommendations Sl. No. 10)

The Committee note that apart from Department of Electronics and Information Technology/Indian Computer Emergency Response Team (CERT-In) there are multiple organisations involved in securing India's cyber space *viz*. Ministry of Defence (MoD), Ministry of Home Affairs, Intelligence Bureau (IB), Department of Telecommunications, National Disaster Management Authority (NDMA), National Technical Research Organisation (NTRO), National Critical Information Infrastructure Protection Centre (NCIIPC), Research and Analysis Wing (RAW), etc. In addition, in order to address effectively the issue of overlapping responsibilities and enhancing coordination between the stakeholder agencies in the country, the Government has approved a framework and has tasked the National Security Council Secretariat (NSCS) to co-ordinate, oversee and ensure compliance of cyber security policies.

The Committee also note that one of the primary challenges facing both Government as well as Industry is to curb the cyber threat at the earliest and this cannot be achieved in isolation by either Government or Industry alone and it requires joint efforts and collaboration. A Joint Working Group (JWG), set up under the chairpersonship of the Deputy National Security Advisor, to work out the details of the Roadmap for cyber security cooperation has inter-alia recommended for setting up of permanent mechanism for Public Private Partnership. While appreciating the initiatives and the coordination of Department of Electronics and Information Technology with various organisations, the Committee recommend the Department to implement the recommendations of the Working Group in a time bound manner.

Reply of the Government

The Joint Working Group set up by National Security Council Secretariat(NSCS) has identified the guiding principles and objectives that would underpin the overall framework and roadmap for Public Private Partnership (PPP) on Cyber Security. It envisages setting up of Institutional Framework, Capacity building in the area of Cyber Security, Development of Cyber Security Standards & Assurance mechanisms, augmentation of testing & certification facilities for Information Technology products. Department is working with NSCS to implement the above recommendations and the action plan for implementation of the recommendations is being worked out.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

MoUs and International Treaties

(Recommendations Sl. No. 12)

The Committee note that the Department has articulated on the need for global cyber jurisprudence in various international fora. The Committee also feel that in this era of inter-dependence and inter-connectivity, a separate discipline of cyber jurisprudence and new international court for cyber jurisprudence is the need of the hour which would go a long way in dealing with threats in cyber space. While admiring the initiatives taken by the Department, the Committee recommend the Department to redouble their efforts in making India a pioneering country for the cause of cyber jurisprudence.

Reply of the Government

Considering the importance of cyber security, the Department is actively working with the Ministry of External Affairs in the area of Global Internet Governance to articulate its concerns and possible ways of enhancing cooperation among countries in dealing with threats in cyber space.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

National Cyber Security Policy-2013

(Recommendations Sl. No. 15)

The Committee note that in order to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country, the Department has prepared 'National Cyber Security Policy (NCSP) – 2013' in consultation with all relevant stakeholders, user entities and public. The aim of the policy is to facilitate creation of secured computing environment and enable adequate trust and confidence in electronic transactions and also guide stakeholders' actions for protection of cyber space. Out of 47 objectives outlined in NCSP-2013, 8 areas have been prioritized by the Department. However, the Committee find it strange to note that NCSP does not depict any deadline/target except for the skilled force and it lacks detailed picture/road map for achieving all the goals of National Cyber Security Policy. On the issue of tentative deadlines by which the rules/guidelines for NCSP-2013 would be in place, the Committee are given to understand that DeitY has already initiated steps to identify the follow up actions as well as agencies responsible and timelines for such actions. The Government is in the process of preparing individual schemes which are to be implemented by the Government and the Joint Working Group set up under the aegis of National Security Council Secretariat (NSCS). Further, the Department has assured to implement major programmes in the next one year. While appreciating the aims and objectives of the NCSP which is definitely a step forward, the Committee urge the Department to chalk out the definite targets/time frame on priority areas with fixing up of responsibilities of different agencies involved/to be involved. The Department should ensure that the micro plans of the Policy are worked out at the earliest and implementation takes off during 2014 itself so as to address the urgent need of dealing with the cyber security threats and the need to build capacity in the country in terms of infrastructure, preventive and protective legal actions, grievance redressal mechanism, evaluation and compliance verification

for imported IT product, certification, awareness, etc. The Department must also ensure that the NCSP-2013 policy which is expected to facilitate creation of secured computing environment and enable adequate trust and confidence for the IT users in the country meets its objectives.

Reply of the Government

In line with the directions of the Cabinet Committee on Security, while approving the National Cyber Security Policy 2013, the Department in association with the National Security Council Secretariat (NSCS) is in the process of identifying actionable points, as well as different agencies responsible for implementation of such actions. Further, as directed by Cabinet Committee on security, Department has identified key projects that are to be initiated in the current year itself. These key initiatives are in support of implementing the National Cyber Security Policy and are related to creation of mechanisms for security threats, early warning and response to security threats.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

Cyber Security and Right to Privacy

(Recommendations Sl. No. 16)

The Committee note that balancing cyber security and right to privacy is extremely complex. The Committee are given to understand that in the absence of any Bill on privacy, the Information Technology Act 2000 as amended in 2008 takes care of data privacy and data protection. The Act contains adequate provisions to deal with various cyber related offenses as well as protection of privacy of individuals. These provisions include Section 43 and section 66 for penalty and stringent punishment for hacking of website, Section 43A - for compensation to the affected person for failure to protect data, Section 72-for penalty for breach of confidentiality and privacy, Section 72A-for punishment for disclosure of information in breach of lawful contract. In addition, The Information Technology Rules (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), 2011 notified on 11th April, 2013 under section 43A of the Information Technology Act defines the sensitive personal data and reasonable security practices and procedures. The Rules require body corporate to provide policy for privacy and disclosure of information (Rule 4), obtain consent of user for collection of information (Rule 5), prior permission required from provider of information before disclosure of sensitive personal information (Rule 6). While the above provisions have been taken note of, the Committee are extremely unhappy to note that the Government is yet to institute a legal framework on privacy. When asked about the status of the above legislation, the Department has diverted the issue stating that the Department of Personnel and Training is still in the process of evolving legislation to address concerns of privacy, in general, and it is still at the drafting stage. The Committee seriously feel that in view of enormous data, very sensitive in nature, being consigned to cyber space each day particularly in the light of Government's visionary UIDAI programme, the Government should not jeopardize the privacy of citizens on the plea that the Department is concerned only with Section 43(A) which it is based on self-regulation. Though the Department has stated that personal information may not come under the purview of DeitY, the Committee are of the opinion that the Department should carry out their responsibilities at least with regard to the digital data. The Committee, while acknowledging the complex nature of the cyber space and the maturity and competence

required in balancing cyber security and right to privacy, desire that the Department in coordination with the Department of Personnel and Training, multi-disciplinary professionals/experts should come out with a comprehensive and people friendly policy which may protect the privacy of citizen and is also foolproof from security point of view.

Reply of the Government

With regard to protection of sensitive personal information, the Information Technology Act 2000, as amended in 2008, contains adequate provisions (Sections 43, 43A,72A and 66) to deal with the aspects of data security as well as protection of sensitive personal information. The Department is participating in consultation process of the Department of Personnel and Training with regard to protection of privacy of citizens.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

Cyber Security and Right to Privacy

(Recommendations Sl. No. 17)

While taking note of the Department's stand on the recent instances of surveillance and interception of data (though only meta-data) by other countries, that incursion into the content of the country's data will not be tolerated, the Committee are of the strong opinion that the Department should have exercised enough caution so that such a situation was not allowed to occur at the first instance. Further, the Committee feel that the Department should be extremely vigilant and cautious in terms of safety as well as in terms of policy with different countries so as to avoid such leakage and interception of sensitive data in the name of surveillance. The Committee, therefore, strongly recommend the Department to take remedial measures and come out with a policy which should be implemented stringently so as to obviate recurrence of such instances.

Reply of the Government

In the wake of concerns regarding US electronic surveillance activities, efforts are being made to enhance country's capacity to protect data and information flows by building better cyber infrastructure and by evolving new cyber security practices. Efforts are also being made towards these objectives by promoting the evolution of better international internet governance-norms, through ongoing discussions at international fora. Framing of e-mail Policy and National Cloud is one such direction,

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

Grievance Redressal Mechanism

(Recommendations Sl. No. 18)

The Committee note that the existing system for registering complaints for grievance redressal regarding cyber-crime involves reporting with the local police stations or cyber-crime cells of law enforcement agencies, however, further redressal process of such cases is similar to other crime related cases. The Committee are given to understand that since Law and Order is a State subject, all actions related to crime including cyber crime are dealt with by respective

States/UTs and relevant data of such cases are being maintained by National Crime Records Bureau (NCRB). Further, many of the States have set up cyber crime cell which are monitoring such crimes. In view of the fact that there is steep rise in cyber-crime instances and the rate at which common man in our country is affected, the Committee are surprised to learn that not all the States have a separate cyber crime cell and there is no centralized system/cell for monitoring cyber-crime. The Committee, therefore, recommend the Department for having mandatory cyber-crime cell not only in each state but also in each District and Block. The Committee also recommend for having a centralized system/cell for monitoring cyber-crime which would have real-time details of registration and disposal status of cyber-crime throughout the country. The Department may also expedite follow up with the Ministry of Home Affairs about the Department's request to increase the awareness among people regarding the mechanism of reporting cyber crime cases with the cyber crime cells of law enforcement agencies.

Reply of the Government

Under the cyber crime investigation program, Ministry of Home Affairs is supporting the establishment of Cyber Crime Police Stations (CCPS) and Cyber Crime Investigations and Forensic Training Facilities (CCIFTF) in each State/UTs of India under Police modernization scheme.

Issues related to cyber crime are under the business domain of Min. of Home Affairs (MHA). Further, Law and Order being a state subject, all actions related to crime including cyber crime are dealt with by respective states/UTs. Many of the states have set up cyber crime cells which are monitoring such crimes. At the national level, relevant data is being maintained by single agency i,e. National Crime Records Bureau (NCRB) under MHA.

On the issue of steps to increase the awareness among people regarding the mechanism of reporting cyber crime cases with the cyber crime cells of law enforcement agencies, the matter had been referred to the Ministry of Home Affairs earlier by this Department on 14th Sept., 2011 and subsequently by Secretary of the Department to Home Secretary on 5th Dec., 2011. Following the observations by the Committee in its 27th Report on the action taken by the Government, Secretary of the Department has once again written to Home Secretary on 7th May, 2012, requesting for necessary steps by MHA in this regard. Department is awaiting a suitable response from MHA on the status of actions and pursuing its efforts for specific actions by MHA.

(Department of Electronics and Information Technology O.M. No. 8(2)/2014-Parl. dated 17.07.2014)

New Delhi;
18 December, 2015
27 Agrahayana, 1937 (Saka)

ANURAG SINGH THAKUR,
Chairperson,
Standing Committee on
Information Technology.

Appendix -I

MINUTES OF THE THIRD SITTING OF THE STANDING COMMITTEE ON INFORMATION TECHNOLOGY (2015-16) HELD ON 18TH DECEMBER, 2015

The Committee sat on Friday, the 18th December, 2015, from 1000 hours to 1040 hours in Committee Room '139', First Floor, Parliament House Annexe, New Delhi.

PRESENT

Shri Anurag Singh Thakur- Chairperson

MEMBERS

Lok Sabha

2. Shri L. K. Advani
3. Shri Prasun Banerjee
4. Dr. Sunil Baliram Gaikwad
5. Shri Hemant Tukaram Godse
6. Shri Virender Kashyap
7. Shri Harinder Singh Khalsa
8. Shri Keshav Prasad Maurya
9. Shri Paresh Rawal
10. Shri Abhishek Singh
11. Smt. R. Vanaroja

Rajya Sabha

12. Shri Salim Ansari
13. Shri Vijay Jawaharlal Darda
14. Shri Meghraj Jain

SECRETARIAT

1.	Shri K. Vijayakrishnan	-	Additional Secretary
2.	Shri J.M. Baisakh	-	Director
3.	Dr. Sagarika Dash	-	Deputy Secretary
4.	Shri Shangreiso Zimik	-	Under Secretary

2. At the outset, the Chairperson welcomed the Members to the sitting of the Committee convened to consider and adopt the following six Draft Action Taken Reports:-

I. Action Taken Report on the Fifty-second Report on the subject 'Cyber Crime, Cyber Security and Right to Privacy';

II. …..xxxxx…….xxxxx…….xxxxx…….xxxxx…….xxxxx…….xxxxx…

III. …..xxxxx…….xxxxx…….xxxxx…….xxxxx…….xxxxx…….xxxxx….

IV. …..xxxxx…….xxxxx…….xxxxx…….xxxxx…….xxxxx…….xxxxx….

V. …..xxxxx…….xxxxx…….xxxxx…….xxxxx…….xxxxx……xxxxx ; and

VI. …..xxxxx…….xxxxx…….xxxxx…….xxxxx…….xxxxx…….xxxxx….

3. The Committee, thereafter, took up for consideration the above Report and after due deliberation adopted the same without any modification.

4. The Committee, then, authorised the Chairperson to present the Action Taken Reports to the House during the current session of Parliament.

The Committee, then, adjourned

*****

…..xxxxx Matter not related to the Report.

Appendix-II

ANALYSIS OF ACTION TAKEN BY THE GOVERNMENT ON THE OBSERVATIONS/ RECOMMENDATIONS CONTAINED IN THEIR FIFTY-SECOND REPORT (FIFTEENTH LOK SABHA)

[Vide Paragraph No. 5 of Introduction]

(i) Observations/ Recommendations which have been accepted by the Government

Rec. Sl. Nos.:- 2,3,6,7,9,11,13,14,20,21 and 22

Total	11
Percentage	50

(ii) Observations/ Recommendations which the Committee do not desire to pursue in view of the replies of the Government

Rec. Sl. Nos.:- Nil

Total	Nil
Percentage	Nil

(iii) Observations/ Recommendations in respect of which replies of the government have not been accepted by the Committee and require reiteration

Rec. Sl. Nos.:-4, 5, and 19.

Total	03
Percentage	13.64

(iv) Observations/ Recommendations in respect of the reply which is of interim nature

Rec. Sl. Nos.:- 1,8,10,12,15,16,17 and 18.

Total	08
Percentage	36.36