XII five-year plan on information technology sector

Report of Sub-Group on Cyber Security

1.0 Background

Over the years, Information Technology has transformed the global economy and connected people and markets in ways beyond imagination. With the Information Technology gaining the centre stage, nations across the world are experimenting with innovative ideas for economic development and inclusive growth. It has also created new vulnerabilities and opportunities for disruption. The cyber security threats emanate from a wide variety of sources and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, security of nation and the stability of the globally linked economy as a whole. The origin of a disruption, the identity of the perpetrator or the motivation for it can be difficult to ascertain and the act can take place from virtually anywhere. These attributes facilitate the use of Information Technology for disruptive activities. As such, cyber security threats pose one of the most serious economic and national security challenges.

2.0 XI Plan – Objectives, targets and achievements

2.1 Objectives and Targets

The following primary objectives had been identified in XI Plan in cyber security:

- Securing cyber space
- Preventing cyber attacks
- Reducing national vulnerability to cyber attacks.
- Minimizing damage and recovery time from cyber attacks
- Capacity building

As such, the cyber security initiatives in the XI plan period had the following focus:

- Enabling Legal Framework
- Security Policy, Compliance and Assurance
- Security R&D
- Security Incident – Early Warning and Response

- National Cyber Alert System
- CERT-In and Sectoral CERTs
- Information Exchange with International CERTs

- Security training
  - Skill & Competence development
  - Domain Specific training – Cyber Forensics, Network & System Security Administration
- Collaboration
  - International
  - National

2.2 Achievements during XI Plan

A number of activities have been performed in each of the above focus areas. Major achievements are summarised below:

2.2.1 Enabling legal framework

Information Technology (Amendment) Act, 2008 has been enacted and rules of important sections have been notified. The provisions of the Information Technology Act deal with evidentiary value of electronic transactions, digital signatures, cyber-crimes, cyber security and data protection.

2.2.2 Security Policy, Compliance and Assurance

Computer Security Guidelines have been circulated to all Departments and Ministries. Cyber security drills are being conducted to assess preparedness of critical organisations. 54 Auditors have been empanelled for audit of IT infrastructure from cyber security point of view.

Crisis Management Plan for countering cyber attacks and cyber terrorism has been released and is being updated annually. Enabling workshops are being conducted in different sectors and states/UTs. Common Criteria (CC) product testing facility has been set up which caters up to level 4 CC certification.

Draft `National Cyber Security Policy' has been prepared and posted on DIT website for public comments.

Controller of Certifying Authority (CCA) has licensed 7 Certifying Authorities (CA). More than 22 lakhs Digital Signature Certificates have been issued. Major Applications using Digital Signatures include e-Procurement for Central and State Govt., e-Tendering, e-Filing of returns (MCA-21), Income Tax filing for corporate and individuals, Inter bank transactions (RTGS and SFMS), E-Filling of Patent Application and NSDL Applications.

2.2.3 Security Incident – Early Warning and Response

A Computer Emergency Response Team –India (CERT-In) has been set up and is operational as the national agency for cyber incidents. It operates a 24x7 Incident Response Help Desk to help users in responding to cyber security incidents. It has been issuing regular alerts on cyber security threats and advises countermeasures to prevent attacks. CERT-In has established linkages with international CERTs and security agencies to facilitate exchange of information on latest cyber security threats and international best practices. CERT-In, in collaboration with CII, NASSCOM and Microsoft, has created a portal "secureyourpc.in" to educate consumers on cyber security issues.

2.2.4 Cyber Security R&D

A number of R&D projects have been supported at premier academic and R&D institutions in the identified Thrust Areas, viz., (a) Cryptography and cryptanalysis, (b) Steganography, (c) Network & systems security assurance, (d) Network Monitoring, (e) Cyber Forensics and (f)Capacity Development in the area of cyber security. A host of Cyber Forensic tools have been developed in the country.

2.2.5 Capacity Development/Training

Training Centres have been set up at CBI, Ghaziabad and Kerala Police to facilitate advanced training in cyber crime investigation. Computer forensic labs and training facilities are being set up in J&K state, North Eastern states. Forensic Centres have been set up with the help of NASSCOM at Mumbai, Bangalore, Bhopal and Kolkata. Virtual training environment based training modules have been prepared. Training has been conducted for Orissa, Delhi, Andhra Pradesh and Karnataka Judicial Officers on Cyber Crime Investigation. 94 training

programmes have been conducted by CERT-In on specialized Cyber Security topics – in which 3392 people have been trained.

2.2.6 Collaboration

As part of National level Cooperation, Cyber security awareness programmes were organised in cooperation with industry associations – CII, NASSCOM-DSCI. MoUs were signed with product and security vendors for vulnerability remediation.

Several activities were undertaken under International Cooperation. International level Cyber security drills were held with Asia –Pacific CERTs. Specific cyber security cooperation agreements were signed with US, Japan and South Korea. India participated in cyber security drills of US (Cyber Storm III). CERT-In experts helped in establishment of CERT-Mauritius. India is participating in Internet traffic scanning in Asia-pacific region. India is a member of UN Committee of Group of Experts as well as in the Council of Security Cooperation in Asia-Pacific (CSCAP) for enhancing cooperation in the area of Cyber Security.

3.0 Current status of Cyber Security preparedness

The initiatives taken by the Government so far have focused on the issues such as cyber security threat perceptions, threats to critical information infrastructure and national Security, protection of critical information infrastructure, adoption of relevant security technologies, enabling legal processes, mechanisms for security compliance and enforcement, Information Security awareness, training and research. These actions have significantly contributed to the creation of a platform that is capable of supporting and sustaining the efforts to securing the cyber space. However, due to the dynamic nature of cyber threat scenario, these actions need to be continued, refined and strengthened from time to time.

Salient features of the results of actions and the level of cyber security preparedness include:

(a) Information Technology (Amendment) Act 2008 has been enacted to cater to the needs of National Cyber Security by addressing host of issues such as technology related cyber crimes, critical information infrastructure protection, data security and privacy protection.

(b) Indian Computer Emergency Response Team (CERT-In) has been operational as a national agency for cyber security incident response. It has established operational linkages with overseas CERTs, and cyber security professional organisations to enhance its ability to respond to the cyber security incidents and take steps to prevent recurrence of the same.

(c) PKI infrastructure, set up to support implementation of Information Technology Act and promote use of Digital Signatures, has enabled the growth and application of digital signature certificates in a number of areas.

(d) National Crisis Management Plan for countering cyber attacks and cyber terrorism has been prepared and is being updated annually. Central Govt. Ministries/Departments and States and UTs as well as organisations in critical sectors are making efforts to prepare and implement their own sectoral Crisis Management Plans.

(e) To enable comprehensive cyber security policy compliance, the Govt. has mandated implementation of security policy within Govt. in accordance with the Information Security Management System (ISMS) Standard ISO 27001. In addition, Computer security guidelines have been issued for compliance within Govt. A Common Criteria based IT product security testing facility has been set up at Kolkata, which can test IT products up to EAL4.

(f) A mechanism for audit and assessment of security posture of Govt. and critical sector organisations has been put in place. Security Auditors have been empanelled for conducting security audits including vulnerability assessment, penetration testing of computer systems and networks of various organizations of the government, critical infrastructure organizations and those in other sectors of the Indian economy. Cyber security drills are being conducted regularly to assess the preparedness of organisations to resist and mitigate cyber attacks.

(g) R&D activities have been supported through premier Academic and R&D Institutions in the country facilitating creation of R&D infrastructure, development skills and solution oriented development.

(h) Nation-wide Information Security Education and Awareness Programme have been in progress to create necessary cyber security awareness through formal and informal programmes. Cyber security training facilities have been set up to provide training to law enforcement agencies and facilitating cyber crime investigation.

4.0 Cyber security – Challenges

The Cyber space is borderless and actions in the cyber space can be anonymous. These features are being exploited by adversaries for perpetration of crime in the cyber space. The scale and sophistication of the crimes committed in the cyber space is continually increasing thereby affecting the citizens, business and Government. As the quantity and value of electronic information have increased, so to have the business models and efforts of criminals and other adversaries who have embraced the cyber space as a more convenient and profitable way of carrying out their activities anonymously.

Today adversaries are producing, selling and distributing malicious code with ease, maximizing their gains and exploiting the fact that attribution is a challenge. Malware is getting stealthier, more targeted, multi-faceted and extremely difficult to analyze and defeat even by the experts in the security field. Organized crime is fast growing and targeting the exponential growth of on line identities and financial transactions. There is increasing evidence of espionage, targeted attacks and lack of traceability in the cyber world as state and non-state actors are compromising, stealing, changing or destroying information and therefore potentially causing risk to national security, economic growth, public safety and competitiveness.

5.0 Cyber Security- Strategic Approach for XII Plan

Cyber Security requirements are quite dynamic that change with the threat environment. Threat landscape needs to be updated regularly to prevent emerging attacks. Collaboration among various agencies is needed to share information regarding emerging threats and vulnerabilities, which would help in effective protection and prevention of cyber attacks.

It is necessary to take a holistic approach to secure Indian Cyber Space. While the cyber security initiatives of the XI plan period will be continued and strengthened, new initiatives will be put in place consistent with emerging threats and evolving technology scenario. The

following Cyber Security strategies are proposed to be adopted during the XII Five Year Plan:

- Enhancing the understanding with respect to factors such as dynamically changing threat landscape, technical complexity of cyber space and availability of skilled resources in the area of cyber security.

- Focus on proactive and collaborative actions in Public-Private Partnership aimed at security incidents prevention, prediction, response and recovery actions and security assurance.

- Enhancing awareness and upgrading the skills, capabilities and infrastructure to protect the country's cyber space, to provide rapid response to cyber attacks, to minimize damage and recovery time and to reduce national vulnerabilities to cyber attacks.

- Improving interaction and engagement with various key stakeholders such as Govt. and critical sector organizations, sectoral CERTs, International CERTs, service providers including ISPs, product and security vendors, security and law enforcement agencies, academia, and media, NGOs and cyber user community.

- Carrying out periodic cyber security mock drills to assess the preparedness of critical sector organizations to resist cyber attacks and improve the security posture.

- Supporting and facilitating basic research, technology demonstration, proof of concept and test bed projects in thrust areas of cyber security through sponsored projects at recognized R&D institutions.

6.0 Key Priorities and Target Deliverables for XII Plan

The cyber security initiatives will be implemented with the following six focus areas during the XII plan period:

(a) Enabling Legal Framework,
(b) Security Policy, Compliance and Assurance,
(c) Security R&D
(d) Security Incident – Early Warning and Response,

(e) Security awareness, skill development and training
(f) Collaboration

The proposed key priorities for implementation and target deliverables in respect of each of the focus areas are given below:

6.1 Enabling Legal Framework

Key Priority

The key priority of this initiative will be up gradation /development of a robust and dynamic legal framework to enable cyber security and address newer cyber crimes.

Target deliverables

It is important to undertake research projects on the theme of cyber laws and related components like, e-commerce, encryption, IPR issues, privacy etc. Further, it is necessary that a data bank/repository of legal cases be created having details of cyber law cases decided in India. Such research projects would help in creating better legal framework and understanding about the issues related to cyber laws including cyber security.

There is a need to devise policy and procedure for obtaining authentic data stored and hosted by Indian companies on servers abroad for lawful access purpose. An encryption/decryption framework is also required keeping in view the concerns of both industry and Law Enforcement Agencies.

As the digital world is much more complex, there is a need to train judiciary, law enforcement agencies and legal practitioners about the cyber crimes, collection of digital evidences and cyber forensics.

With the ever-growing reliance on technology and spurt in newer forms of cyber crimes, it becomes imperative to introduce courses on cyber law.

In line with the requirements, the target deliverables include:

- Suitable amendments to existing legal framework
- Strengthening enforcement mechanism

- Capacity building for judiciary, law enforcement agencies, legal practitioners and students

6.2 Security Policy, Compliance and Assurance

Key priority

Cyber security policy compliance and assurance initiative needs to focus on creating an enabling mechanism for achieving conformance with provisions of IT Act, statutes and other policy initiatives of the Government and regulatory bodies.

Target deliverables

With the growing use of IT, there is an increasing need to generate and sustain user's confidence in the IT systems and transactions. Accordingly, simultaneous efforts are needed on the part of Govt., business and industry in terms of enabling frameworks, mechanisms for compliance and assurance. On its part, the Government is making efforts to identify the core services that need to be protected from cyber attacks and is seeking to work with organizations responsible for these systems so that their services are secured in a way that is proportional to the threat perception. Industry and critical infrastructure organizations have started to focus on their ability to gain users confidence through improved software development, security engineering practices and the adoption of strengthened security models and best practices.

Most often, users of IT products depend on inputs from others to know about the security of the product. There is a need to have a mechanism to certify IT products to provide assurance from security point of view. This in turn requires creation of standards for conformance, establishment of acceptable evaluation method and process to certify products and at the same time ensure that privacy is maintained as per the prevailing regulations. This is required both for proprietary and open source products.

With India emerging as a leading outsourcing partner, there is a need to address compliance requirements to international standards and best practices on security and privacy. As such, there is a requirement for a comprehensive assurance framework that enables compliance within the country and provides assurance on compliance to out sourcing organizations and rest of the world.

The target deliverables include:

- Annual cyber security studies and surveys related to compliance and assurance
- Enhancement of crisis management plan and emergency preparedness
- Enhancement of security audit, assessment and certification infrastructure (Third party certification, Self-certification, empanelment and ratings of auditors, technical security testing, cyber security drills),
- Mechanism for generating a national cyber security index leading to national risk management framework
- Enhancement of IT product technical security assurance mechanism (Common Criteria security test/evaluation & Crypto Module Validation Program)

6.3 Cyber Security Research & Development

Key priority

The key priority of this initiative will be to carry out innovative R&D with focus on basic research, technology development and demonstration, setting up test-beds, transition, diffusion and commercialisation leading to widespread deployment.

Target deliverables

Indigenous R&D efforts are essential for facilitating the creation of a sound S&T environment. Resources like skilled manpower and infrastructure created through pre-competitive public funded projects provide much needed inputs to entrepreneurs to be globally competitive through further R&D. Indigenous R&D efforts will contribute to creation of knowledge and expertise to face new and emerging security challenges and to produce cost-effective, tailor-made indigenous security solutions. Indigenous efforts are also required to develop products which are not available from outside sources due to export restrictions.

Viable industry-academic/R&D interactions are vital for implementation of the activities. Joint R&D programme in specific identified projects in Public Private Partnership mode will need to be explored. These joint projects are expected to speed up the development efforts and make available outcome from such joint projects for commercial exploitation and deployment in relatively short period of time. This joint R&D programme also will

help in harnessing the technical skills and capabilities of institutions and organisations in public and private sector.

The target deliverables include:

- Setting up of Centres of excellence in Cryptography, Malware Research, Mobile Security and Cyber Forensics
- Creation of Centre for technology transfer and facilitating prototype to production of products
- Programs to focus on cryptography, cryptanalysis, algorithm design/ development/ hardware realisation
- Attack detection, protection, response, recovery and prevention systems
- Security solutions for cloud environment
- Mobile security solutions
- Embedded systems security particularly addressing security requirements in SCADA systems
- Cyber security assurance framework for Govt sector

6.4 Security Incident - Early Warning and Response

Key priority

The key priority is strengthening National Cyber Alert System for rapid identification and response to security incidents and information exchange to all desired elements that are critical for cyber security, to reduce the risk of cyber threat and resultant effects.

Target deliverables

Information systems must be able to operate while under attack and also have the resilience to restore full operations in their wake. Towards this end, rapid identification, information exchange, and remediation are necessary to contain a security incident and mitigate the damage caused by malicious cyberspace activity. With the active involvement of critical infrastructure organizations, public and private institutions, a National Cyber Alert System can perform requisite analysis, conduct watch and warning activities, enable information exchange, and facilitate restoration efforts.

CERT-In is operational and is catering to the security needs of Indian Cyber community. In line with the emerging requirements, there is a need to further augment the facilities at CERT-In in terms of manpower, communication systems, tools, etc. for vulnerability prediction, analysis and mitigation, cyber forensics analysis, cyber space monitoring/ interception and critical information infrastructure security. For an effective National Cyber Security Alert System, there is a need to create/upgrade sectorial CERTs to cater to the very specific domain needs of different sectors.

Strengthening of Government Cyber Security infrastructure

The Government agencies need to set an example in the development and use of secure computer and communication networks. There is a need for priority action to strengthen the security of the Government IT infrastructure to facilitate faster and efficient information flow between various user agencies within the Government as well as effective interface with users outside the Government. In order to meet the upcoming challenges in securing the Government IT infrastructure, adequate attention should be paid to the use of appropriate technology and applications and development of suitable information security policies and guidelines.

The target deliverables include:

- Establishment of Threat, Vulnerability and Malware Research Centre
- Expansion of CERT-In Operations
- Building sensor/honeypot networks at key ICT installations
- Creation of a central knowledge repository
- Incident and response mechanism at national gateways
- Security Information Sharing and Analysis Centres (ISACs)

  Cyber Security Operational Centre (CSOC) which will have co-ordination role with necessary authority and accountability in respect of cyber security defense measures
- Establishment of Regional level Cyber Security Help Desks
- Establishment of Botnet Cleaning Centres in the Govt., critical infrastructure and public sector organizations.

6.5 Security Awareness, Skill Development and Training

Key priority

The key priority is to establish cyber security capacity building and training mechanisms for developing a strong and dynamic cyber security skilled work force and a cyber vigilant society.

Target deliverables

Building appropriate human resources is vital to address upcoming security challenges and threats. There is a need to have trained manpower at different levels both in the Government and private sector. It would also be important to create interest among good IT students by creating opportunities for them. Also those who are already on the job need to be retrained and their skills upgraded. There is a need to include cyber security curriculum both at school and college levels.

Mass awareness campaign is important to create cyber security awareness among citizens. The promotion and publicity campaign could include (a) Seminars, exhibitions, contests etc., (b) Radio and TV programmes, (c) Videos on specific topics, (d) Web casts, Podcasts, (e) Leaflets and Posters and (f) Suggestion and Award Schemes.

The local law enforcement agencies at the operational level as well as central law enforcement agencies are required to be equipped to deal with cyber crimes. There is a need for creating awareness and impart training to law enforcement agencies and judiciary regarding IT Act provisions, cyber security aspects, cyber crime investigation procedures and cyber forensics. A separate Centre of Excellence may need to be created for this purpose.

Indigenous certification programmes need to be evolved to enable affordable certification and generating certified cyber security manpower.

The target deliverables include:

- Launch of Security Education, Skill Building and Awareness Programme
- Sustained awareness campaign through electronic media

- Establishment of Cyber Security Training Labs/facilities across the country
- Establishment of examination, accreditation & certification infrastructure
- Establishment of Cyber Security Concept Labs, Digital Cyber Forensic Training Labs, Cyber Security Auditing of Assurance Labs, SCADA/embedded security labs
- Establishment of Centre of Excellence for capacity building for Law Enforcement Agencies and Judiciary

6.6 Collaboration

Key priority

The key priority is to promote shared understanding and leverage relationships for furthering the cause of security of cyber space.

Target Deliverables

The cyber threat sources and attacks span across countries. As such there is a need to enhance global cooperation among security agencies, CERTs and Law Enforcement agencies of various countries to effectively mitigate cyber threats. Accordingly, it is vital to have well-developed Cyber Security collaborative framework established through different government agencies in broad collaboration with private sector, partners and stakeholders in academia, national and international agencies. In this context, DIT should coordinate and be a focal point for all cyber security matters including critical sector in the civilian sector for effective collaboration and interface for cyber security aspects.

Target deliverables include :

- Security cooperation arrangements with overseas CERTs and industry
- Proactive engagement at UN and Asia-Pacific level
- Enhanced information sharing mechanism within the country
- Focused and sustained engagement program for law enforcement agencies and judiciary
- Creation of a tiered structure for information sharing
- Establishment of a think tank for cyber security policy inputs, discussion and deliberations

7.0 Implementation Plan

The activities to be carried out during the course of implementation of XII plan under each of the six focus areas are indicated in the following paragraphs.

7.1 Enabling Legal Framework

Studies will need to be carried out to understand the impact of new technology, crime trends and current policies on the business environment, public safety, national security and global competitiveness. Studies are also necessary on international cyber laws to harmonise Indian cyber laws with laws prevailing internationally. Based on the studies carried out, amendments required in the existing legal framework will have to be identified and appropriate means devised to strengthen the enforcement mechanism. Policies and procedures will have to be framed based on appropriate public inputs and debates. An enabling legal framework will require:

- Policy and framework to establish data sovereignty, ownership and control
- Legal framework for encryption in the backdrop of cyber security, privacy and national security
- Framework for lawful access in India with defined checks and balances and redressal mechanism
- Legal framework for usage of surveillance technologies for public safety
- Framework to protect privacy of online users
- Enabling mechanism / framework for cyber security assistance to law enforcement agencies (to take care of costs of additional equipment needed for lawful access).

Activities to create awareness about the role of CERT-In, Adjudicating Officers & Cyber Appellate Tribunal as an Authority under the Information Technology Act, 2000 will need to be undertaken. Efforts will have to be made to set standards for forensic tools and procedures in India.

7.2 Security Policy, Compliance and Assurance

The activities needed to be pursued include

- Development of crypto module validation program and operationalisation,
- Enhancement of technical capability of Common Criteria Test lab in emerging technology,

- Implementation of IT product technical security assurance program and operationalisation,
- Updation of crisis management plan,
- Enablement of development and implementation of sectoral crisis management plans,
- Carrying out periodic cyber security mock drills to assess the preparedness of critical sector organizations to resist cyber attacks,
- Establishing institutional platform for security professionals in the country,
- Publishing guidelines and mandate for secure development and deployment of ICT systems,
- Creating a mechanism for interface between the government and public on policy compliance and assurance like interactive portal, website, etc., and
- Establishing a mechanism for incentivising security compliance and assurance.

7.3 Cyber Security R&D

The R&D Programs undertaken have to address all aspects of development: Study of the security properties of existing major systems and components, development of prototypes in selected application and infrastructure domains and simulation environments, development of deployable systems, testing of the systems developed and deployment and maintenance of trustworthy systems throughout the life cycle.

An indicative list of areas of R&D is given below:

- Indigenous cryptographic algorithms, protocols and systems for securing data at storage and transmission
- Quantum Cryptography Research
- Secure software engineering and development
- Trusted/trustworthy systems development with end-to-end security
- Tamper resistant and self healing systems
- Static and dynamic roots of trust for secure transactions
- Device security
- System-on-chip security
- Predicting future resilience of systems
- Solutions for ensuring trust of electronic transactions
- Video analytics
- Analysis and certification of commercial IT Systems
- Software assurance, code testing and analysis
- Threat Management systems

- Active devices with built-in capability for event based monitoring
- Network penetration and vulnerability assessment tools
- Interception of encrypted communication
- Development of national security index leading to national risk management framework
- Development of compliance and self-assessment tools, validation and implementation.

7.4 Security Incident - Early Warning and Response

The activities needed to be pursued under this initiative include

- Augmenting operating capabilities of CERT-In to address rising scale and scope of national security incident response management,
- Adopting and deploying state-of-art tools and techniques,
- Creating a structured knowledge repository with continuous streaming of information,
- Strengthening partnership and cooperation with security technology industry, international CERTs and security forums,
- Acquisition of intelligence about vulnerabilities, threats, and security risks collated from a comprehensive list of sources,
- Building of framework for engaging external expertise,
- Establishing a mechanism for technical security posture measurement,
- Establishing Security knowledge management delivery mechanism, and
- Establishing a collaboration platform for engaging with security community.

7.5 Security Awareness, Skill Development and Training

The activities needed to be undertaken under this initiative include

- Building capacity through various training delivery modes and certifications in network security, forensics, audit, security management and application security,
- Mandating Certification for security roles including CISO/CSO and those involved with critical information infrastructure,
- Enhancing Cyber Security Training and Awareness Programmes in different States across the country,
- Conducting Security Training and courses in Public Private Partnership mode,
- Conducting, supporting and enabling Cyber Security Workshops/Seminars and Certifications,

- Conducting security awareness programmes at schools level with suitable cyber security curriculum,
- Introducing specific and specialized courses in University, Engineering colleges and management institutions,
- Promoting Secure Coding Practices,
- Creating and updating role relevant standardised courseware contents,
- Establishing Centre of Excellence for capacity development of judiciary and law enforcement agencies, and
- Development of courseware on cyber law and cybercrime investigation and implementation.

7.6 Collaboration

The activities necessary under this initiative will include

- Developing bilateral and multi-lateral relationships in the area of cyber security with other countries,
- Creating models for collaborations and engagement with all relevant stakeholders,
- Enabling private-to-private and private-to-government collaboration and cooperation in the area of cyber security for sharing information on practices and breaches,
- Actively contributing to the development of international standards,
- Collaboratively conducting cyber drills and actively participating in international exercises including promoting global priority group,
- Engaging in defining controls for managing supply chain risks,
- Collaborating for bot-net takedowns and increasing consumer trust in ICT, and
- Seeking international legal cooperation by entering into bilateral/multilateral Protocols or Conventions on Cyber Crimes and Cyber Security.

8.0 Institutional arrangement and role of DIT

DIT will act as a nodal agency to implement the cyber security activities planned for the XII Plan. It will provide funding support to the programs for execution by partner agencies. Public private partnership (PPP) arrangement will need to be explored in the relevant areas like joint funding of select R&D projects, organizing awareness and training programs jointly with industry associations, state governments etc.

9.0 Summary of Recommendations

The primary objectives identified in the XI Plan for securing country's cyber space, viz. preventing cyber attacks, reducing national vulnerability to cyber attacks, reducing national vulnerability to cyber attacks, and minimizing damage and recovery time from cyber attacks, continue to be valid for the XII plan period. Accordingly, the cyber security focus areas in the XII plan period will be (a) Enabling Legal Framework, (b) Security Policy, Compliance and Assurance, (c) Security R&D, (d) Security Incident – Early Warning and Response, (e) Security awareness, skill development and training, and (f) Collaboration.

New initiatives recommended to be taken up in the XII Plan include:

- Seamless integration of agencies involved in the area of cyber security
- Creating Centres of Excellence for research in identified areas of advanced security.
- Setting up security threats, vulnerability and malware analysis facility.
- Setting up a mechanism to certify IT products to provide security assurance (including creation of standards, establishment of evaluation methods and processes and facility to certify products).
- Establishing Security Information Sharing and Analysis Centres (ISACs) across the regions and sectors for government-to-private and private-to-private information sharing.
- Establishing Sectoral CERTs.
- Strengthening infrastructure and activities at CERT-In.
- Strengthening National Cyber Alert System for rapid identification and response to security incidents and information exchange.
- Setting up Cyber Security Help Desks at regional levels for general users to provide first level of guidance and support.
- Setting up Botnet Cleaning Centres in the Government, Public, and Critical Infrastructure Sectors.
- Establishing Cyber Security Training Labs/facilities across the country in collaboration with State Governments and Private Sector

Some of the major targets/deliverables in the identified focus areas of the XII Plan are as follows:

- **Enabling Legal Framework -** Setting up of think tanks in Public-Private mode to identify gaps in the existing policy and frameworks and take action to address them. This includes addressing privacy concerns of on-line users.

- **Security Policy, Compliance and Assurance-** Enhancement of IT product security assurance mechanism (Common Criteria security test/evaluation, ISO 15408 & Crypto Module Validation Program), establishing a mechanism for national cyber security index leading to national risk management framework.

- **Security R&D** - Creation of Centres of Excellence in identified areas of advanced Cyber Security R&D and Centre for Technology Transfer to facilitate transition of R&D prototypes to production, supporting R&D projects in thrust areas.

- **Security Incident - Early Warning and Response-** Comprehensive threat assessment and attack mitigation by means of net traffic analysis and deployment of honey pots, development of vulnerability database.

- **Security awareness, skill development and training -** Launching formal Security Education, Skill Building and Awareness Programmes.

- **Collaboration -** Establishing a collaborative platform/ think-tank for cyber security policy inputs, discussion and deliberations, operationalisation of security cooperation arrangements with overseas CERTs and industry, and seeking legal cooperation of international agencies on cyber crimes and cyber security.