ANNEXURES

I. Discussion draft on National Cyber Security Policy Department Of Information Technology
II. National Cyber Security Policy (NCSP), 2013
III. XII Five-Year Plan on Information Technology Sector - Report of Sub-Group on Cyber Security
IV. Members of the Global Forum on Cyber Expertise, Hague, Netherlands 2015
V. The Hague Declaration on GFCE
VI. Framework Document GFCE
Discussion draft

on

National Cyber Security Policy

“For secure computing environment and adequate trust & confidence in electronic transactions”

Your comments/feedback on this document are most welcome. Please send your valuable comments/feedback by 15 May 2011 to Dr Gulshan Rai, Director General, CERT-In, at the above address or on email id ‘grai@mit.gov.in’
National Cyber Security Policy

"For secure computing environment and adequate trust & confidence in electronic transactions"

Contents

1.0 Security of Cyber Space – Strategic perspective 3
   1.1 IT as an engine for economic growth and prosperity 3
   1.2 Security of cyber space - Need for action 3
   1.3 Target audience 3
   1.4 Securing cyber space – Key policy considerations 4

2.0 Cyber space – Nature of threat 4
   2.1 Threat landscape 4
   2.2 International cooperation 5
   2.3 Securing cyber space – Scope of action 5
      2.3.1 Cyber security and cyber defense 5
      2.3.2 Cyber intelligence and cyber defense 5
   2.4 Priorities for action 6
   2.5 Partnership and collaborative efforts 7

3.0 Enabling processes 7
   3.1 Security threat and vulnerability management 7
   3.2 Security threat early warning and response 8
   3.3 Security best practices - compliance and assurance 9
   3.4 Security crisis management plan for countering cyber attacks and cyber terrorism 12
   3.5 Security legal framework and law enforcement 12
   3.6 Security information sharing and cooperation 13

4.0 Enabling technologies – Deployment and R&D 13
   4.1 Deployment of technical measures 14
   4.2 Security research and development 14

5.0 Enabling people 15
   5.1 Security education and awareness 15
   5.2 Security skills training and certification 16
   5.3 Security training infrastructure 16

6.0 Responsible actions by user community 16
   6.1 Actions by Network service providers 16
   6.2 Actions by Large Corporates 17
   6.3 Actions by small/medium users and home users 17
National Cyber Security Policy

“For secure computing environment and adequate trust & confidence in electronic transactions”

Annexure I - Stakeholder agencies

1 National Information Board (NIB) 18
2 National Crisis Management Committee (NCMC) 18
3 National Security Council Secretariat (NSCS) 18
4 Ministry of Home affairs 18
5 Ministry of Defence 18
6 Department of Information Technology (DIT) 18
7 Department of Telecommunications (DoT) 19
8 National Cyber Response Centre - Indian Computer Emergency Response Team (CERT-In) 19
9 National Information Infrastructure Protection Centre (NIIPC) 19
10 National Disaster Management of Authority (NDMA) 19
11 Standardisation, Testing and Quality Certification (STQC) Directorate 19
12 Sectoral CERTs 20
1.0 Security of Cyber Space – Strategic perspective

1.1. IT as an engine for economic growth and prosperity

The IT sector has become one of the most significant growth catalysts for the Indian economy. In addition to fuelling India’s economy, this sector is also positively influencing the lives of its people through direct and indirect contribution to the various socio-economic parameters such as employment, standard of living and diversity among others. The sector has played a significant role in transforming India’s image to that of a global player in providing world-class technology solutions and business services. The government has been a key driver for increased adoption of IT-based products and solutions in the country. It has embarked on various IT-enabled initiatives including in Public services (Government to citizen services, citizen identification, public distribution systems), Healthcare (telemedicine, remote consultation, mobile clinics), Education (e-Learning, virtual classrooms, etc) and Financial service (mobile banking/payment gateways), etc. In addition, Government sector has enabled increased IT adoption in the country through sectors reforms that encourage IT acceptance and National programmes such as National eGovernance Programmes (NeGP) and the Unique Identification Development Authority of India (UIDAI) programme that create large scale IT infrastructure and promote corporate participation.

1.2 Security of cyber space - Need for action

In light of the growth of IT sector in the country, ambitious plans for rapid social transformation & inclusive growth and India’s prominent role in the IT global market, providing right kind of focus for secure computing environment and adequate trust & confidence in electronic transactions becomes one of the compelling priorities for the country. This kind of focus enables creation of suitable cyber security eco system in the country, in tune with globally networked environment and at the same time assures its citizens as well the global community about the seriousness of its intentions and ability to act suitably.

1.3 Target audience

The cyber security policy is an evolving task, which need to be regularly updated/refined in line with technological trends and security challenges posed by such technology directions. This policy caters for the whole spectrum of ICT users and providers including small and home users, medium and large enterprises and Government & non-Government entities. It provides an overview of what it takes to effectively protect information, information systems & networks and also to provide an insight into the Government’s approach and strategy for protection of cyber space in the country. It also outlines some pointers to enable collaborative working of all key players in public & private to safeguard country’s information and information systems. This policy, therefore, aims to create a cyber security framework, which will address all the related issues over a long period. The framework will lead to specific actions and programmes to enhance the security posture of country’s cyber space.
1.4 Securing cyber space – Key policy considerations

The key considerations for securing the cyber space include:

- The security of cyber space is not an optional issue but an imperative need in view of its impact on national security, public safety and economic well-being.
- The issue of cyber security needs to move beyond traditional technological measures such as anti-virus and firewalls. It needs to be dynamic in nature and have necessary depth to detect, stop and prevent attacks.
- Cyber security intelligence forms an integral component of security of cyber space in order to be able to anticipate attacks, adopt suitable counter measures and attribute the attacks for possible counter action.
- Effective correlation of information from multiple sources and real-time monitoring of assets that need protection and at the same time ensuring that adequate expertise and process are in place to deal with crisis situations.
- There is a need to focus on having a suitable security posture and adopt counter measures on the basis of hierarchy of priority and understanding of the inter dependencies, rather than attempting to defend against all intrusions and attacks.
- Security is all about what people, process and technology and as such there is a clear need for focusing on people and processes while attempting to use the best available technological solutions, which otherwise could prove ineffective.
- Use of adequately trained and qualified manpower along with suitable incentives for effective results in a highly specialized field of cyber security.
- Security needs to be built-in from the conceptual design stage itself when it comes to developing and deploying critical information infrastructure, as opposed to having security as an afterthought.

2.0 Cyber space – Nature of threat

2.1 Threat landscape

Existing and potential threats in the sphere of cyber security are among the most serious challenges of the 21st century. Threats emanate from a wide variety of sources, and manifest themselves in disruptive activities that target individuals, businesses, national infrastructures, and governments alike. Their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole. Malicious use of information technology can easily be concealed. The origin, identity of the perpetrator, or motivation for the disruption can be difficult to ascertain. Often, the perpetrators of these activities can only be inferred from the target, the effect or other circumstantial evidence. Threat actors can operate with substantial impunity from virtually anywhere. The motives for disruption vary widely, from simply demonstrating technical prowess, to the theft of money or information, or as an extension of state conflict. The source of these threats includes non-state actors such as criminals and, potentially, terrorists as well as States themselves. Many malicious tools and methodologies originate in the
efforts of criminals and hackers. The growing sophistication and scale of criminal activity increases the potential for harmful actions.

2.2 International cooperation

Increasingly, nations are also concerned that the ICT supply chain could be influenced or subverted in ways that would affect normal, secure and reliable use of information technology. Inclusion of malicious hidden functions in information technology can undermine confidence in products and services, erode trust in commerce, and affect national security. As disruptive activities using information technology grow more complex and dangerous, it is obvious that no nation is able to address these threats alone. Confronting the challenges of the 21st century depends on successful cooperation among like-minded partners. Collaboration among nations, and between nations, the private sector and civil society, is important and the effectiveness of measures to improve cyber security requires broad international cooperation.

2.3 Securing cyber space – Scope of action

2.3.1 Cyber security and cyber defense

Cyber security is the activity of protecting information and information systems (networks, computers, data bases, data centers and applications) with appropriate procedural and technological security measures. In that sense, the notion of cyber security is quite generic and encompasses all protection activities. Cyber defense relates to a much more specialized activity linked to particular aspects and organizations. The distinguishing factors between cyber security and cyber defense in a network environment are the nature of the threat, the assets that need to be protected and the mechanisms applied to ensure that protection. Cyber defense relates to defensive actions against activities primarily originating from hostile actors that have political, quasi-political or economic motivation that have an impact on national security, public safety or economic well being of the society. The cyber defense environment requires deployment of technologies and capabilities for real-time protection and incident response. Generally, cyber defense is driven by intelligence on the threat to achieve the kind of defense that directs, collects, analysis and disseminates the relevant actionable intelligence information to the stakeholders concerned for necessary proactive, preventive and protective measures. The effectiveness of cyber defense lies in the proactive nature of security counter measures as well as in ensuring resilience and continuity of operations, despite the possibilities of successful attacks.

2.3.2 Cyber intelligence and cyber defense

The value of collecting intelligence information about threat sources and possible cyber attacks cannot be underestimated. A well-deployed cyber attack can yield vital information that compromises communication and encryption ciphers. It tends to project the power of the attacker and demoralize the victim. However, the changing phase of cyber attacks as well as ever-increasing sophistication of attack methods have complicated the efforts of collecting valuable intelligence information for effective proactive, preventive and protective measures. Generally, attacks directed against Govt. and critical information infrastructure can be categorized as either
massive attacks, aimed at disabling the infrastructure rendering it unusable or inaccessible to users; or targeted attacks, aimed at collecting sensitive/strategic information. Massive attacks generally take the form of denial of service attacks against the infrastructure. The targeted attacks involve a good deal of customization and personalization of attack methods and levels of technological and operational sophistication. Skillful execution of attack and the methodology used to conceal any traces of attack complicates the task of advance intelligence information collection and/or attack detection.

2.4 Priorities for action

Assuring security of cyber space requires careful and due attention to creation of well defined systems and processes, use of appropriate technology and more importantly, engaging right kind of people with suitable awareness, ethics and behavior. Considering the transnational character of information technology & the cyber space, the technical & legal challenges in ensuring security of information, information systems & networks as well as related impact on socio-economic life in the country, the priorities for action for creating a secure cyber eco-system include series of enabling processes, direct actions and cooperative & collaborative efforts within the country and beyond, covering:

- **Creation of necessary situational awareness regarding threats to ICT infrastructure for determination and implementation of suitable response**
- **Creation of a conducive legal environment in support of safe and secure cyber space, adequate trust & confidence in electronic transactions, enhancement of law enforcement capabilities that can enable responsible action by stakeholders and effective prosecution**
- **Protection of IT networks & gateways and critical communication & information infrastructure**
- **Putting in place 24 x 7 mechanism for cyber security emergency response & resolution and crisis management through effective predictive, preventive, protective, response and recovery actions**
- **Policy, promotion and enabling actions for compliance to international security best practices and conformity assessment (product, process, technology & people) and incentives for compliance.**
- **Indigenous development of suitable security techniques & technology through frontier technology research, solution oriented research, proof of concept, pilot development etc. and deployment of secure IT products/processes**
- **Creation of a culture of cyber security for responsible user behavior & actions**
- **Effective cyber crime prevention & prosecution actions**
- **Proactive preventive & reactive mitigation actions to reach out & neutralize the sources of trouble and support for creation of global security eco system, including public-private partnership arrangements, information sharing, bilateral & multi-lateral agreements with overseas CERTs, security agencies and security vendors etc.**
- **Protection of data while in process, handling, storage & transit and protection of sensitive personal information to create a necessary environment of trust.**
2.5 Partnership and collaborative efforts

Government leadership catalyzes activities of strategic importance to the Nation. In cyber security, such leadership can energize a broad collaboration with private-sector partners and stakeholders to generate fundamental technological advances in the security of the Nation’s IT infrastructure. First, in support of national and economic security, the Government should identify the most dangerous classes of cyber security threats to the Nation, the most critical IT infrastructure vulnerabilities, and the most difficult cyber security problems. Second, the Government can use these findings to develop and implement a coordinated R&D effort focused on the key research needs that can only be addressed with such leadership. While these needs will evolve over time, this cyber security policy provides a starting point for such an effort. Public-private partnership is a key component of this cyber security policy. These partnerships can usefully confront coordination problems. They can significantly enhance information exchange and cooperation. Public-private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery operations. These actions will help in leveraging rapid technological developments and capabilities of private sector.

3.0 Enabling processes

3.1 Security threat and vulnerability management

All infrastructure facilities face a certain level of risk associated with various threats. These threats may be result of natural events, accidents or intentional acts to cause harm. Regardless of the nature of the threat, facility owners have a responsibility to limit or manage risks from these threats to the extent possible. This is more so, if the facility is a part of nation’s critical information infrastructure. As such focus of these efforts would be:

1) To prevent cyber attacks on critical ICT infrastructure
2) Reduce vulnerability of critical ICT infrastructure to cyber attacks.
3) Enhancing the capability of critical ICT infrastructure to resist cyber attacks
4) Minimize damage and recovery in a reasonable time frame

The key actions to reduce security threats and related vulnerabilities are:

1) Identification and classification of critical information infrastructure facilities and assets.
2) Roadmaps for organization-wise security policy implementation in line with international security best practices standards and other related guidelines.
3) Process for national level security threat & vulnerability assessments to understand the potential consequences.
4) Use of secure products/services, protocols & communications, trusted networks and digital control systems. Internet Service Providers (ISPs) would be closely associated in providing for secure information flow through their networks and gateways. Appropriate legally binding agreements need to be in place to support law enforcement, information security incident handling and crisis management processes on a 24x7 basis.
5) Identification of national level security organization (CERT-In, DIT) to act as a nodal agency and co-ordinate all matters related to information security in the country, with clearly defined roles & responsibilities.

6) Emergency preparedness and crisis management (Mirror Centers, Hot/warm/cold sites, communication, redundancy, and disaster recovery plans, test & evaluation of plans etc)

7) Periodic as well as random verification of the level of emergency preparedness of critical information infrastructure facilities in resisting cyber attacks and minimize damage & recovery time in case cyber attacks do occur.

8) Development of comprehensive repair and maintenance policy so as to minimize false alarms and increase cyber resource availability to all users efficiently.

3.2 Security threat early warning and response

a) National cyber alert system

(i) Rapid identification, information exchange, and remediation can often mitigate the damage caused by malicious cyberspace activity. For these activities to take place effectively at a national level, it requires a central nodal agency (CERT-In, DIT) to perform analysis, issue warnings, and coordinate response efforts. Because no information security plan can be impervious to concerted and intelligent attacks, information systems must be able to operate while under attack and also have the resilience to restore full operations in reasonable time frame. The National Cyber Alert System will involve critical infrastructure organizations, public and private institutions to perform analysis, conduct watch and warning activities, enable information exchange, and facilitate restoration efforts.

(ii) The essential actions under National Cyber Alert System include:
   - Identification of focal points in the critical infrastructure
   - Establishment of a public-private architecture for responding to national-level cyber incidents
   - Tactical and strategic analysis of cyber attacks and vulnerability assessments
   - Expanding the Cyber Warning and Information Network to support the role of Government in coordinating crisis management for cyberspace security;
   - Cyber security drills and exercises in IT dependent business continuity plans of critical sectors to assess the level of emergency preparedness of critical information infrastructure facilities in resisting cyber attacks and minimize damage & recovery time in case cyber attacks do occur.

b) Sectoral CERTS

In order to effectively deal with targeted cyber attacks on sensitive and strategic sectors, it is essential to operationalise sectoral CERTs in all identified critical sectors such as finance, defence, energy, transportation, telecommunication etc. These CERTs would be responsible for all coordination and communication actions within their respective sectors and should be in regular touch with CERT-In for any incidence resolution support as well as dealing with cyber crisis requiring broader action.
c) Local incident response teams
Each critical sector organisation should have an identified team of personnel who will be part of
the respective local Incident Response Team. This team would:
- Identify the correctness of the severity level of any incident
- Contain, Eradicate and Recover
- Seek necessary resources and support from the corresponding Level II Incident
  Resolution Team
- Provide regular updates to higher management regarding progress of the incident
  handling process
- Escalate to an expert team/sectoral CERT or CERT-In, if unable to resolve within the
  prescribed time frame/reasonable time frame.

3.3 Security best practices - compliance and assurance
(i) Critical Information Infrastructure Protection
The primary focus of these efforts is to secure the information resources belonging to Government
as well as those in the critical sectors. The critical sectors include Defence, Finance, Energy,
Transportation and Telecommunications. Consequently, many in the industry and critical
infrastructure organizations have come to recognize that their continued ability to gain consumer
confidence will depend on improved software development, systems engineering practices and
the adoption of strengthened security models and best practices. The designated agency of the
Government would coordinate the efforts towards protection of critical information infrastructure in
the country and enable development of expertise in communication, interception, monitoring and
early warning, and surprise vulnerability checks with due authorization.

(a) Implementation of security best practices in Govt. and Critical sectors
In order to reduce the risk of cyber attacks and improve upon the security posture of critical
information infrastructure, Government and critical sector organizations are required to do the
following on priority:
1) Identify a member of senior management, as Chief Information Security Officer (CISO),
knowledgeable in the nature of information security & related issues and designate him/her as a
‘Point of contact’, responsible for coordinating security policy compliance efforts and to regularly
interact with the Indian Computer Emergency Response Team (CERT-In), Department of
Information Technology (DIT), which is the nodal agency for coordinating all actions pertaining to
cyber security
2) Prepare information security plan and implement the security control measures as per
international security best practices standards and other guidelines, as appropriate
3) Carry out periodic IT security risk assessments and determine acceptable level of risks,
consistent with criticality of business/functional requirements, likely impact on business/functions
and achievement of organisational goals/objectives.
4) Periodically test and evaluate the adequacy and effectiveness of technical security control
measures implemented for IT systems and networks. Especially, Test and evaluation may
become necessary after each significant change to the IT applications/systems/networks and can
include, as appropriate the following:
   – Penetration Testing (both announced as well as unannounced)
Vulnerability Assessment
– Application Security Testing
– Web Security Testing

5) Carry out Audit of Information infrastructure on an annual basis and when there is major upgradation/change in the Information Technology Infrastructure, by an independent IT Security Auditing organization

6) Report to CERT-In cyber security incidents, as and when they occur and the status of cyber security, periodically

(b) Government networks
The government agencies need to set an example in the development and use of secure computer and communication networks. For this purpose, a part of departmental budget should be earmarked for IT and information security needs. Besides this, all ministries/departments and other agencies of the government should ensure that they take necessary precautions and steps to promote the culture of information security amongst their employees and attached agencies. Necessary change in office procedure should be undertaken to bring in vogue, reliable and robust paperless offices where required. Top-level management of government departments should pay attention to the development of suitable information security policy and guidelines and encourage the use of appropriate technology and applications in the organization.

(c) Government secure intranet
There is a need for priority action to create a countrywide secure intranet for connecting strategic installations with CERT-In as the nodal center for emergency response and coordination. This intranet will facilitate faster and efficient information sharing between strategic installations and CERT-In as well as supporting crisis management and disaster recovery during national IT security emergencies.

(ii) Information security Assurance Framework
In order to ensure implementation security best practices in critical sector organizations and periodic verification of compliance, there is a need to create, establish and operate a ‘Information security Assurance Framework’, including creation of national conformity assessment infrastructure. Information security Assurance Framework is aimed at assisting National level efforts in protecting critical information infrastructure. It supports Government, Critical Infrastructure Organizations and other key IT users of nation's economy through series of “Enabling and Endorsing” actions.

(a) Enabling actions are essentially Promotional/Advisory/Regulatory in nature and involve publication of “National Security Policy Compliance requirements” and cyber security guidelines and supporting documents to facilitate cyber security implementation and compliance.

b) Endorsing actions are part of national conformity assessment infrastructure. These are essentially commercial in nature and may involve more than one service provider offering commercial services after having fulfilled requisite qualification criteria and demonstrated ability prior to empanelment. These include:
National Cyber Security Policy

“For secure computing environment and adequate trust & confidence in electronic transactions”

- **Assessment and certification** of compliance to international IT security best practices, standards and guidelines (Ex. ISMS certification, Trusted company certification for Data security and privacy protection, IS system audits, Penetration testing/Vulnerability assessment etc)

  Government and critical infrastructure organizations can make use of CERT-In evaluated and empanelled third party agencies for their organisation/site specific IT security assessment services (including ISMS assessment, risk assessment, network security profiling, penetration testing, vulnerability assessment, application security testing etc) under specific contract and pre-determined rules of engagement. Contact details of the agencies empanelled by CERT-In are available at 'http://www.cert-in.org.in’

- **IT Security product evaluation and certification** as per accepted international standards

  These actions provide an assurance that the process of specification, implementation and evaluation of a IT security product has been conducted in a rigorous and acceptable manner.

- **IT security manpower training, qualification** and other related services to assist user in IT security implementation and compliance.

(c) **Data security and privacy protection for ‘Trust and Confidence’**

In order to stay competitive in the global marketplace, business entities have to continually generate adequate levels of trust & confidence in their services in terms of privacy and data protection through the use of internationally accepted best practices and ability to demonstrate where necessary.

(d) **Quality and protection of electronic records**

Organizations need to ensure that important data/records are protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements. Where a follow-up action against a person or organization involves legal action (either civil or criminal), electronic evidence needs to be properly collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). It is a good practice to have audit logs recording user activities, exceptions, and information security events and retained for an agreed period to assist in future investigations.

(iii) **E-governance**

All e-governance initiatives in the country should be based on best information security practices. Government should encourage wider usage of Public Key Infrastructure (PKI) in its own departments. There is a need to empanel Information Security professionals/ organizations to assist E-Governance initiatives and monitor quality of their performance/service through appropriate quality standards.

(iv) **Secure software development and application**

Software development process, whether in-house or outsourced, needs to be supervised and monitored using a system development life cycle methodology that includes information security considerations and selection of appropriate security controls and countermeasures.
(a) Open standards
To minimize the risk of dependency on proprietary IT products, open standards need to be encouraged. A consortium of government and private sector needs to be created for enhancing the use of validated and certified IT products based on open standards.

3.4 Security crisis management plan for countering cyber attacks and cyber terrorism

The Crisis Management Plan for Countering Cyber Attacks and Cyber Terrorism outlines a framework for dealing with cyber related incidents for a coordinated, multi-disciplinary and broad based approach for rapid identification, information exchange, swift response and remedial actions to mitigate and recover from malicious cyber related incidents impacting critical national processes. The Crisis Management Plan for Countering Cyber Attacks and Cyber Terrorism describes the following aspects:

- The Critical Sectors, Nature of cyber crisis and possible targets and impact of particular type of crisis on these targets.
- Focused cyber attacks affecting the organisations in critical sector such as Defence, Energy, Finance, Space, Telecommunications, Transport, Public Essential Services and Utilities, Law Enforcement and Security would lead to national crisis.
- Different types of cyber crisis described include Large-scale defacement and semantic attacks on websites, Malicious code attacks, Large scale SPAM attacks, Spoofing, Phishing attacks, Social Engineering, Denial of Service (DoS) and Distributed DoS attacks, attacks on DNS, Applications, infrastructure and Routers, Compound attacks and High Energy RF attacks.
- Incident prevention and precautionary measures to be taken at organisational level which include implementation of Information Security Best Practices based on ISO 27001 standard, Business Continuity Plan, Disaster Recovery, Security of Information and Network, Security Training and Awareness, Incident Management, Sharing of information pertaining to incidents and conducting mock drills to test the preparedness of Critical Infrastructure organisations to withstand cyber attacks.

3.5 Security legal framework and law enforcement

3.5.1 A sound legal framework and effective law enforcement procedures are essential in deterring cyber-crime. In this direction, recent amendments to the Indian IT ACT 2000 provide for an excellent means to enable adequate trust and confidence in the online environment and enhance law enforcement capability to deal effectively with cyber crime. Besides this, for greater international cooperation, there is a need to harmonize national laws and enforcement procedures. Priorities for action include:

- Dynamic legal framework that is in tune with the technological changes and international developments in the area of information security (Ex. Electronic signatures, national encryption policy etc)
- Dedicated cyber-crime units with skilled and competent manpower
National Cyber Security Policy

“For secure computing environment and adequate trust & confidence in electronic transactions”

- Dedicated state-of-the-art facilities for law enforcement for cyber crime prevention and prosecution
- Dedicated state-of-the-art training facilities for law enforcement and judiciary to assist them in keeping track with developments
- International cooperation agreements facilitating sharing of information and crime prosecution

3.5.2 Combating Hi-Tech Crime/Cyber Crime

The Hi-Tech Crime/Cyber Crime covers any crime committed against or using IT systems including hacking, web site defacements, identity theft, stealing personal information, Internet fraud or online child abuse. Criminals have sought to exploit the Internet as it offers a rapid and productive means of communicating as well as a good chance of anonymity. Although the threats in cyber space are similar to those in the physical space (be it theft, fraud or terrorism), IT has changed the way in which these activities are perpetrated. The Hi-Tech/Cyber Crime strategy aims to focus on issues such as e-crime reporting, crime reduction and prevention, legislation, response, role of business-industry-public and international cooperation.

3.6 Security information sharing and cooperation

The cyber threat sources and attacks span across countries. As such, as there is a need for enhanced global cooperation among security agencies, CERTs and Law Enforcement agencies of various countries to effectively mitigate cyber threats and be able to respond to information security incidents in a timely manner.

The priorities for international cooperation are:
- Information security and Information Assurance Technology to prevent, protect against, detecting, responding, and recovering from cyber attacks in critical information infrastructure that may have large-scale consequences.
- Collaboration in training personnel for implementing and monitoring secure government intranets and cyber space
- Joint R&D projects in frontline and futuristic technologies
- Coordination in early warning, threat & vulnerability analysis and incident tracking
- Information security drills/exercises to test the vulnerability & preparedness of critical sectors

4.0 Enabling technologies – Deployment and R&D

4.1 Deployment of technical measures

Many different types of threats exist in the cyber world, but these threats will fall into three basic categories - un-authorized access, impersonation and denial of service. These threats may usually result in eavesdropping and information theft, disabling access to network resources (DOS attacks), un-authorized access to system and network resources and data manipulation.
The selection and effective implementation of cyber security technologies require adequate consideration of a number of key factors, including:

- Implementing technologies through a layered, defense-in-depth strategy;
- Considering organizations’ unique information technology infrastructure needs when selecting technologies;
- Utilizing results of independent testing when assessing the technologies’ capabilities;
- Training staff on the secure implementation and utilization of these technologies; and
- Ensuring that the technologies are securely configured.

The organizations in Govt. and critical sector may consider protecting their networks, systems and data through deployment of access control technologies (for perimeter protection, authentication and authorization), system integrity measures, cryptography mechanisms and configuration management and assurance.

4.2 Security research and development

4.2.1 Indigenous R&D is an essential component of national information security measures due to various reasons- a major one being export restrictions on sophisticated products by advanced countries. Second major reason for undertaking R&D is to build confidence that an imported IT security product itself does not turn out to be a veiled security threat. Other benefits include creation of knowledge and expertise to face new and emerging security challenges, to produce cost-effective, tailor-made indigenous security solutions and even compete for export market in information security products and services. Success in technological innovation is significantly facilitated by 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. Private sector is expected to play a key role in meeting needs of short term R&D leading to commercially viable products. Besides in-house R&D, this sector may find it attractive to undertake collaborative R&D with leading research organizations.

4.2.2 Issues for focused action in R&D are information security functional Requirements, securing the Infrastructure, domain-Specific Security Needs and enabling Technologies for R&D.

4.2.3 The Thrust areas of R&D include:

- Cryptography and cryptanalysis research and related aspects
- Network Security – including wireless & Radio (WiFi, WiMax, 3G, GPRS)
- System Security including Biometrics
- Security architecture
- Monitoring and Surveillance
- Vulnerability Remediation & Assurance
- Cyber Forensics
- Malware Analysis Tools
- Scalable trust worth systems and networks
- Identity Management
Department Of Information Technology

National Cyber Security Policy

“For secure computing environment and adequate trust & confidence in electronic transactions”

- Situational understanding and Attack attribution
- Survivability of critical systems and networks.

5.0 Enabling people
5.1 Security education and awareness

5.1.1 Many cyber vulnerabilities exist because of lack of information security awareness on the part of computer users, system/network administrators, technology developers, auditors, Chief Information Officers (CIOs), Chief Executive Officers (CEOs), and Corporates. A lack of trained personnel and the absence of widely accepted, multi-level certification programs for information security professionals complicate the task of addressing cyber vulnerabilities. This policy identifies following major actions and initiatives for user awareness, education, and training:
  - Promoting a comprehensive national awareness program
  - Fostering adequate training and education programs to support the Nation’s information security needs (Ex School, college and post graduate programs on IT security)
  - Increase in the efficiency of existing information security training programs and devise domain specific training programs (ex: Law Enforcement, Judiciary, E-Governance etc)
  - Promoting private-sector support for well-coordinated, widely recognized professional information security certifications.

5.1.2 Information security awareness promotion is an ongoing process. The main purpose is to achieve the broadest penetration to enhance awareness and alert larger cyber community in cases of significant security threats. The promotion and publicity campaign could include
  - Seminars, exhibitions, contests etc
  - Radio and TV programmes
  - Videos on specific topics
  - Web casts, Pod casts
  - Leaflets and Posters
  - Suggestion and Award Schemes

5.1.3 Safe use of IT for children and small & home users

Owing to the vulnerability of children and small & home users on the Internet for criminal exploitation, special campaigns are required to promote acceptable and safe use information technology. This combines the knowledge of the needs of protection while understanding the power of information technology. In addition, campaigns may also be directed to raise the awareness among the parents about the means of helping children to go online safely.

5.2 Security skills training and certification

Information security requires many skilled professionals to deal with variety of domain specific actions. In order to train security professionals with appropriate skill sets, it is necessary to identify and create a pool of master trainers and training organizations to cater to specific set of training requirements such as security audits, Management and information assurance, Technical
Department Of Information Technology

National Cyber Security Policy

“For secure computing environment and adequate trust & confidence in electronic transactions”

operations etc. These trainers and training organizations would then train and certify professionals for deployment in critical sectors. The following are some of the professional cyber security roles that can be targeted for training and certification:

- Chief information security officer (CISO)
- System operations and maintenance personnel
- Network security specialists
- Digital forensics and incident response analysis
- Implementation of information security and auditing
- Vulnerability analyst
- Information security systems and software development
- Acquisition of technology
- Techno-legal
- Law enforcement

5.3 Security training infrastructure

The requirement of security professionals is very huge and is only bound to increase with more and more of ICT usage. Towards this effect, it is an imperative need to set up adequate training infrastructure to cater to the needs of all types of users, particularly law enforcement agencies, judicial officers, owners/operators of e-Government services etc. This effort may also involve large number of private organizations to have an effective outreach.

6.0 Responsible actions by user community

Essentially, actions for securing information and information systems are required to be done at different levels within the country. Besides the actions by Government, other stakeholders such as network services providers (ISP), large corporates and small users/home users are also required to be play their part to enhance the security of cyber space within the country.

6.1 Actions by Network service providers

- Compliance to international security best practices, service quality and service level agreements (SLAs) and demonstration.
- Pro-active actions to deal with and contain malicious activities, ensuring quantity of services and protecting average end users by way of net traffic monitoring, routing and gateway controls.
- Keeping pace with changes in security technology and processes to remain current (configuration, patch and vulnerability management)
- Conform to legal obligations and cooperate with law enforcement activities including prompt actions on alert/advisories issued by CERT-in
- Use of secure product and services and skilled manpower
- Crisis management and emergency response.
6.2 Actions by Large Corporates
• Compliance to international security best practices and demonstration
• Pro-active actions to deal with and contain malicious activities, and protecting average end users by say of net traffic monitoring, routing and gateway controls
• Keeping pace with changes in security technology and processes to remain current (configuration, patch and vulnerability management)
• Conform to legal obligations and cooperate with law enforcement activities including prompt actions on alert/advisories issued by CERT-In
• Use of secure product and services and skilled manpower
• Crisis management and emergency response.
• Periodic training and up gradation of skills for personnel engaged in security related activities
• Promote acceptable users’ behavior in the interest of safe computing both within and outside.

6.3 Actions by small/medium users and home users
• Maintain a level of awareness necessary for self-protection
• Use legal software and update at regular intervals.
• Beware of security pitfalls while on the net and adhere to security advisories as necessary
• Maintain reasonable and trust-worthy access control to prevent abuse of computer resources.
Stakeholder agencies

1 National Information Board (NIB)
National Information Board is an apex agency with representatives from relevant Departments and agencies that form part of the critical minimum information infrastructure in the country. NIB is entrusted with the responsibility of enunciating the national policy on information security and coordination on all aspects of information security governance in the country. NIB is headed by the National Security Advisor.

2 National Crisis Management Committee (NCMC)
The National Crisis Management Committee (NCMC) is an apex body of Government of India for dealing with major crisis incidents that have serious or national ramifications. It will also deal with national crisis arising out of focused cyber attacks. NCMC is headed by the Cabinet Secretary and comprises of Secretary level officials of Govt. of India. When a situation is being handled by the NCMC it will give directions to the Crisis Management Group of the Central Administrative Ministry/Department as deemed necessary.

3 National Security Council Secretariat (NSCS)
National Security Council Secretariat (NSCS) is the apex agency looking into the political, economic, energy and strategic security concerns of India and acts as the secretariat to the NIB.

4 Ministry of Home Affairs (MHA)
Ministry of Home Affairs issues security guidelines from time to time to secure physical infrastructure. The respective Central Administrative Ministries/Departments and critical sector organizations are required to implement these guidelines for beefing up/strengthening the security measures of their infrastructure. MHA sensitizes the administrative departments and organizations about vulnerabilities and also assists the respective administrative Ministry/Departments.

5 Ministry of Defence
Ministry of Defence is the nodal agency for cyber security incident response with respect to Defence sector. MoD, IDS (DIARA), formed under the aegis of Headquarters, Integrated Defence Staff, is the nodal tri-Services agency at the national level to effectively deal with all aspects of Information Assurance and operations. It has also formed the Defence CERT where primary function is to coordinate the activities of services/MoD CERTs. It works in close association with CERT-In to ensure perpetual availability of Defence networks.

6 Department of Information Technology (DIT)
Department of Information Technology (DIT) is under the Ministry of Communications and Information Technology, Government of India. DIT strives to make India a global leading player in Information Technology and at the same time take the benefits of Information Technology to every walk of life for developing an empowered and inclusive society. It is mandated with the task of dealing with all issues related to promotion & policies in electronics & IT.
National Cyber Security Policy

“For secure computing environment and adequate trust & confidence in electronic transactions”

7 Department of Telecommunications (DoT)
Department of Telecommunications (DoT) under the Ministry of Communications and Information Technology, Government of India, is responsible to coordinate with all ISPs and service providers with respect to cyber security incidents and response actions as deemed necessary by CERT-In and other government agencies. DoT will provide guidelines regarding roles and responsibilities of Private Service Providers and ensure that these Service Providers are able to track the critical optical fiber networks for uninterrupted availability and have arrangements of alternate routing in case of physical attacks on these networks.

8 National Cyber Response Centre - Indian Computer Emergency Response Team (CERT-In)
CERT-In monitors Indian cyberspace and coordinates alerts and warning of imminent attacks and detection of malicious attacks among public and private cyber users and organizations in the country. It maintains 24x7 operations centre and has working relations/collaborations and contacts with CERTs, all over the world; and Sectoral CERTs, public, private, academia, Internet Service Providers and vendors of Information Technology products in the country. It would work with Government, Public & Private Sectors and Users in the country and monitors cyber incidents on continuing basis through out the extent of incident to analyse and disseminate information and guidelines as necessary. The primary constituency of CERT-In would be organizations under public and private sector domain.

9 National Information Infrastructure Protection Centre (NIIPC)
NIIPC is a designated agency to protect the critical information infrastructure in the country. It gathers intelligence and keeps a watch on emerging and imminent cyber threats in strategic sectors including National Defence. They would prepare threat assessment reports and facilitate sharing of such information and analysis among members of the Intelligence, Defence and Law enforcement agencies with a view to protecting these agencies’ ability to collect, analyze and disseminate intelligence. NIIPC would interact with other incident response organizations including CERT-In, enabling such organizations to leverage the Intelligence agencies’ analytical capabilities for providing advanced information of potential threats.

10 National Disaster Management of Authority (NDMA)
The National Disaster Management Authority (NDMA) is the Apex Body for Disaster Management in India and is responsible for creation of an enabling environment for institutional mechanisms at the State and District levels. NDMA envisions the development of an ethos of Prevention, Mitigation and Preparedness and is striving to promote a National resolve to mitigate the damage and destruction caused by natural and man-made disasters, through sustained and collective efforts of all Government agencies, Non-Governmental Organizations and People’s participation.

11 Standardisation, Testing and Quality Certification (STQC) Directorate
STQC is a part of Department of Information Technology and is an internationally recognized Assurance Service providing organization. STQC has established nation-wide infrastructure and developed competence to provide quality assurance and conformity assessment services in IT
National Cyber Security Policy

“For secure computing environment and adequate trust & confidence in electronic transactions”

Sector including Information Security and Software Testing/Certification. It has also established a test/evaluation facility for comprehensive testing of IT security products as per ISO 15408 common criteria security testing standards.

12 Sectoral CERTs
Sectoral CERTs in various sectors such as Defence, Finance (IDRBT), Railways, Petroleum and Natural Gas, etc, would interact and work closely with CERT-In for mitigation of crisis affecting their constituency. Sectoral CERTs and CERT-In would also exchange information on latest threats and measures to be taken to prevent the crisis.
File No: 2(35)/2011-CERT-In

Ministry of Communication and Information Technology
Department of Electronics and Information Technology

NOTIFICATION

Dated: 6 July, 2013

Subject: Notification on National Cyber Security Policy-2013 (NCSP–2013)


Preamble

1. Cyberspace¹ is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.

2. Owing to the numerous benefits brought about by technological advancements, the cyberspace today is a common pool used by citizens, businesses, critical information infrastructure, military and governments in a manner that makes it difficult to draw clear boundaries among these different groups. The cyberspace is expected to be more complex in the foreseeable future, with many fold increase in networks and devices connected to it.

3. Information Technology (IT) is one of the critical sectors that rides on and resides in cyberspace. It has emerged as one of the most significant growth catalysts for the Indian economy. In addition to fuelling India’s economy, this sector is also positively influencing the lives of its people through direct and indirect contribution to the various socio-economic parameters such as employment, standard of living and diversity among others. The sector has played a significant role in transforming India’s image to that of a global player in providing world-class technology solutions and IT business services. The government has been a key driver for increased adoption of IT-based products and IT enabled services in Public services (Government to citizen services, citizen identification, public distribution systems), Healthcare (telemedicine, remote consultation, mobile clinics), Education (e-Learning, virtual classrooms, etc) and Financial services (mobile banking / payment gateways), etc. Such initiatives have enabled increased IT adoption in the country through sectoral reforms and National programmes which have led to creation of large scale IT infrastructure with corporate / private participation.

4. In the light of the growth of IT sector in the country, ambitious plans for rapid social transformation & inclusive growth and India’s prominent role in the IT global market, providing right kind of focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks, has become one of the compelling priorities for the

¹ISO / IEC 27032-2012
country. Such a focus enables creation of a suitable cyber security eco-system in the country, in tune with globally networked environment.

5. Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation-states and non-state actors. Cyber attacks that target the infrastructure or underlying economic well-being of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures. A cyber related incident of national significance may take any form; an organized cyber attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity. Some of the examples of cyber threats to individuals, businesses and government are identity theft, phishing, social engineering, hactivism, cyber terrorism, compound threats targeting mobile devices and smart phones, compromised digital certificates, advanced persistent threats, denial of service, bot nets, supply chain attacks, data leakage, etc. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

6. There are various ongoing activities and programs of the Government to address the cyber security challenges which have significantly contributed to the creation of a platform that is now capable of supporting and sustaining the efforts in securing the cyber space. Due to the dynamic nature of cyberspace, there is now a need for these actions to be unified under a National Cyber Security Policy, with an integrated vision and a set of sustained & coordinated strategies for implementation.

7. The cyber security policy is an evolving task and it caters to the whole spectrum of ICT users and providers including home users and small, medium and large enterprises and Government & non-Government entities. It serves as an umbrella framework for defining and guiding the actions related to security of cyberspace. It also enables the individual sectors and organizations in designing appropriate cyber security policies to suit their needs. The policy provides an overview of what it takes to effectively protect information, information systems & networks and also gives an insight into the Government’s approach and strategy for protection of cyber space in the country. It also
outlined some pointers to enable collaborative working of all key players in public & private to safeguard country's information and information systems. This policy, therefore, aims to create a cyber security framework, which leads to specific actions and programmes to enhance the security posture of country's cyber space.

I. Vision

To build a secure and resilient cyberspace for citizens, businesses and Government

II. Mission

To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

III. Objectives

1) To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.

2) To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).

3) To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.

4) To enhance and create National and Sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.

5) To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources.

6) To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, pilot development, transition, diffusion and commercialisation leading to widespread deployment of secure ICT
products / processes in general and specifically for addressing National Security requirements.

7) To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.

8) To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.

9) To provide fiscal benefits to businesses for adoption of standard security practices and processes.

10) To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cyber crime or data theft.

11) To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.

12) To create a culture of cyber security and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.

13) To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.

14) To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

IV. Strategies

A. Creating a secure cyber ecosystem

1) To designate a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities.

2) To encourage all organizations, private and public to designate a member of senior management, as Chief Information Security Officer (CISO), responsible for cyber security efforts and initiatives.

3) To encourage all organizations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices. Such policies should include establishing standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis
management plan, proactive security posture assessment and forensically enabled information infrastructure.

4) To ensure that all organizations earmark a specific budget for implementing cybersecurity initiatives and for meeting emergency response arising out of cyber incidents.

5) To provide fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cybersecurity.

6) To prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cybersecurity compliance and proactive actions.

7) To establish a mechanism for sharing information and for identifying and responding to cybersecurity incidents and for cooperation in restoration efforts.

8) To encourage entities to adopt guidelines for procurement of trustworthy ICT products and provide for procurement of indigenously manufactured ICT products that have security implications.

B. Creating an assurance framework

1) To promote adoption of global best practices in information security and compliance and thereby enhance cybersecurity posture.

2) To create infrastructure for conformity assessment and certification of compliance to cybersecurity best practices, standards and guidelines (Eg. ISO 27001 ISMS certification, IS system audits, Penetration testing / Vulnerability assessment, application security testing, web security testing).

3) To enable implementation of global security best practices in formal risk assessment and risk management processes, business continuity management and cyber crisis management plan by all entities within Government and in critical sectors, to reduce the risk of disruption and improve the security posture.

4) To identify and classify information infrastructure facilities and assets at entity level with respect to risk perception for undertaking commensurate security protection measures.

5) To encourage secure application/software development processes based on global best practices.

6) To create conformity assessment framework for periodic verification of compliance to best practices, standards and guidelines on cybersecurity.
C. Encouraging Open Standards

1) To encourage use of open standards to facilitate interoperability and data exchange among different products or services.

2) To promote a consortium of Government and private sector to enhance the availability of tested and certified IT products based on open standards.

D. Strengthening the Regulatory framework

1) To develop a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space (such as cloud computing, mobile computing, encrypted services and social media) and its harmonization with international frameworks including those related to Internet governance.

2) To mandate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to regulatory framework.

3) To enable, educate and facilitate awareness of the regulatory framework.

E. Creating mechanisms for security threat early warning, vulnerability management and response to security threats

1) To create National level systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

2) To operate a 24x7 National Level Computer Emergency Response Team (CERT-In) to function as a Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management. CERT-In will function as an umbrella organization in enabling creation and operationalization of sectoral CERTs as well as facilitating communication and coordination actions in dealing with cyber crisis situations.

3) To operationalise 24x7 sectoral CERTs for all coordination and communication actions within the respective sectors for effective incidence response & resolution and cyber crisis management.
4) To implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national processes or endangering public safety and security of the Nation, by way of well coordinated, multi disciplinary approach at the National, Sectoral as well as entity levels.

5) To conduct and facilitate regular cyber security drills & exercises at National, sectoral and entity levels to enable assessment of the security posture and level of emergency preparedness in resisting and dealing with cyber security incidents.

F. Securing E-Governance services

1) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan for all e-Governance initiatives in the country, to reduce the risk of disruption and improve the security posture.

2) To encourage wider usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.

3) To engage information security professionals / organisations to assist e-Governance initiatives and ensure conformance to security best practices.

G. Protection and resilience of Critical Information Infrastructure

1) To develop a plan for protection of Critical Information Infrastructure and its integration with business plan at the entity level and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

2) To Operate a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) to function as the nodal agency for critical information infrastructure protection in the country.

3) To facilitate identification, prioritisation, assessment, remediation and protection of critical infrastructure and key resources based on the plan for protection of critical information infrastructure.

4) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan by all critical sector entities, to reduce the risk of disruption and improve the security posture.

5) To encourage and mandate as appropriate, the use of validated and certified IT products.
6) To mandate security audit of critical information infrastructure on a periodic basis.

7) To mandate certification for all security roles right from CISO / CSO to those involved in operation of critical information infrastructure.

8) To mandate secure application / software development process (from design through retirement) based on global best practices.

H. Promotion of Research & Development in cyber security

1) To undertake Research & Development programs for addressing all aspects of development aimed at short term, medium term and long term goals. The Research & Development programs shall address all aspects including development of trustworthy systems, their testing, deployment and maintenance throughout the life cycle and include R&D on cutting edge security technologies.

2) To encourage Research & Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of cyber security challenges and target for export markets.

3) To facilitate transition, diffusion and commercialisation of the outputs of Research & Development into commercial products and services for use in public and private sectors.

4) To set up Centres of Excellence in areas of strategic importance for the point of security of cyber space.

5) To collaborate in joint Research & Development projects with industry and academia in frontline technologies and solution oriented research.

I. Reducing supply chain risks

1) To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices.

2) To build trusted relationships with product / system vendors and service providers for improving end-to-end supply chain security visibility.

3) To create awareness of the threats, vulnerabilities and consequences of breach of security among entities for managing supply chain risks related to IT (products, systems or services) procurement.
J. Human Resource Development

1) To foster education and training programs both in formal and informal sectors to support the Nation’s cyber security needs and build capacity.

2) To establish cyber security training infrastructure across the country by way of public private partnership arrangements.

3) To establish cyber security concept labs for awareness and skill development in key areas.

4) To establish institutional mechanisms for capacity building for Law Enforcement Agencies.

K. Creating Cyber Security Awareness

1) To promote and launch a comprehensive national awareness program on security of cyberspace.

2) To sustain security literacy awareness and publicity campaign through electronic media to help citizens to be aware of the challenges of cyber security.

3) To conduct, support and enable cyber security workshops / seminars and certifications.

L. Developing effective Public Private Partnerships

1) To facilitate collaboration and cooperation among stakeholder entities including private sector, in the area of cyber security in general and protection of critical information infrastructure in particular for actions related to cyber threats, vulnerabilities, breaches, potential protective measures, and adoption of best practices.

2) To create models for collaborations and engagement with all relevant stakeholders.

3) To create a think tank for cyber security policy inputs, discussion and deliberations.

M. Information sharing and cooperation

1) To develop bilateral and multi-lateral relationships in the area of cyber security with other countries.

2) To enhance National and global cooperation among security agencies, CERTs, Defence agencies and forces, Law Enforcement Agencies and the judicial systems.
To create mechanisms for dialogue related to technical and operational aspects with industry in order to facilitate efforts in recovery and resilience of systems including critical information infrastructure.

N. Prioritized approach for Implementation

To adopt a prioritized approach to implement the policy so as to address the most critical areas in the first instance.

V. Operationalisation of the Policy

This policy shall be operationalised by way of detailed guidelines and plans of action at various levels such as national, sectoral, state, ministry, department and enterprise, as may be appropriate, to address the challenging requirements of security of the cyberspace.

New Delhi, Dated: 2 July 2013

Copy to:
1. All Concerned Ministries/Departments of Government of India
2. Cabinet Secretariat
3. PMO
4. Planning Commission
5. Comptroller and Auditor General of India
6. JS & FA, Department of Electronics and Information Technology
7. Internal Distribution

Page 10 of 10
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 outsourcing 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.
### Members of the Global Forum on Cyber Expertise

**18 May 2015**

1. African Union
2. Argentina
3. Australia
4. Belgium
5. Bangladesh
6. Canada
7. Chile
8. Cisco
9. Council of Europe
10. Estonia
11. European Union
12. Europol
13. Finland
14. France
15. Germany
16. Hewlett Packard
17. Huawei Technologies
18. Hungary
19. India
20. International Chamber of Commerce
21. International Telecommunication Union
22. Israel
23. Japan
24. Kenya
25. Microsoft
26. Morocco
27. Mexico
28. The Netherlands
29. New Zealand
30. Norway
31. NRD CS
32. Organization of American States
33. Republic of Korea
34. Romania
35. Rwanda
36. Senegal
37. Sweden
38. Switzerland
39. Symantec Corporation
40. Turkey
41. Ukraine
42. United Kingdom
43. United States of America
44. Vietnam
45. Vodafone
Launch of the Global Forum on Cyber Expertise

16 April 2015

The Hague Declaration on the GFCE

1. Today, we, governments, intergovernmental organisations and private companies, meet to launch the Global Forum on Cyber Expertise. We recognise and welcome that societies are becoming increasingly digitized, interconnected and dependent on the cyber domain for communication, innovation and sustainable social development and economic growth. We acknowledge that this creates opportunities that should be accessible for every individual worldwide.

2. To fully reap the benefits of information and communication technology, further investments are needed to ensure a free, open and secure cyberspace. As a consequence, inclusive and greater collaboration in the area of capacity building and exchange of expertise within the cyber domain is rapidly becoming one of the most important topics on the international cyber agenda, as was also noted in the 2013 Seoul Framework for and Commitment to Open and Secure Cyberspace.

3. As societies need to rapidly develop their capacity to take full advantage of cyberspace and need to overcome evolving challenges presented in this field, we all face financial and human resource constraints. We need to find better and smarter ways to work together by fostering existing and building new partnerships, establishing best practices and providing assistance to one another.

4. We stand committed to strengthening this cooperation on cyber by creating more opportunities for governments, the private sector, civil society, the technical community and academia from various regions of the world to engage and develop innovative solutions to this truly global challenge. We recognise the growing number of players in the field with relevant cyber experience and expertise, and we seek to make best use of these assets through closer cooperation.

5. We emphasise the need to strengthen and reinforce the existing framework of international cooperation and build new partnerships, enhance institutional capacity where it is most needed. We seek to develop a mutually reinforcing relationship with relevant multilateral institutions and develop practitioner networks that will have an enduring impact on global cyber capacity.

6. As a concrete sign of our unified and firm commitment to strengthen cyber capacity and expertise and to make the existing international cooperative efforts in this field more effective, we hereby establish the Global Forum on Cyber Expertise (hereinafter: GFCE).

Objectives

7. The GFCE will create a pragmatic, action-oriented and flexible forum. It will be consistent with, complement and reinforce existing bilateral, multilateral, multi-party, regional and international efforts to build cyber capacity and expertise and avoid duplication and overlap. The efforts undertaken within the framework of the GFCE will be consistent with international law, in particular the Charter of the United Nations, and respect the Universal Declaration of Human Rights, the
International Covenant on Civil and Political Rights and the UN Guiding Principles on Business and Human Rights, where appropriate.

8. The GFCE’s overarching and long term goal is to strengthen cyber capacity and expertise globally.

9. To this end, the GFCE’s primary objective is to provide a dedicated, informal platform for policymakers, practitioners and experts from different countries and regions to facilitate:

   a) Sharing experience, expertise, best practices and assessments on key regional and thematic cyber issues. The initial focus areas for capacity and expertise building are cyber security, cybercrime, data protection and e-governance;
   b) Identifying gaps in global cyber capacity and develop innovative solutions to challenges;
   c) Contributing to existing efforts and mobilise additional resources and expertise to build global cyber capacity in partnership with and according to the particular needs of interested countries, upon their request.

10. Acknowledging that our participation in the GFCE is voluntary and not a legally binding commitment, we have established a framework document that will allow the GFCE to operate in a flexible, transparent and inclusive manner.

11. We plan to hold a high level meeting every year, in which we will discuss the achievements within the GFCE, including Initiatives taken, share experiences and lessons learned, and decide upon the way forward, preferably within the margins of the Global Conferences on Cyberspace. Non-members are welcome to take part in the discussions during these meetings. Civil society, the technical community and academia will be encouraged to participate and contribute to these discussions.

12. A small administrative unit will provide secretarial, communications and logistical support, and will prepare, in coordination with future hosts of the Global Conferences on Cyberspace, the annual high level meeting. This secretariat will initially be hosted and financed by the Netherlands.
Launch of the Global Forum on Cyber Expertise

16 April 2015

Framework Document

Purpose

1. This Framework Document outlines the structure and operation of the Global Forum on Cyber Expertise (hereinafter: “GFCE”). It reflects the shared understanding of its members that the GFCE should be structured in a way that is voluntary, complementary, inclusive and resource driven. Activities are focused on identifying and addressing key geographic and thematic cyber issues.

2. Furthermore, it ensures the GFCE will remain a flexible, action-oriented and consultative forum that can evolve to meet contemporary challenges in cyberspace. It will complement the efforts already being undertaken in the field of cyber capacity and expertise building on a bilateral, multilateral, multi-party, regional and international level and avoid duplication and overlap. The GFCE seeks to develop a mutually reinforcing relationship with relevant multilateral institutions. This Framework Document should be seen in juncture with the The Hague Declaration on the GFCE, which outlines the objectives and values upon which the GFCE is based.

Members

3. Participation in the GFCE is voluntary. The GFCE is an informal forum, with no authority to take legally binding decisions. Neither this Framework Document nor participation in the GFCE more generally imposes any legal obligations on members.

4. The GFCE is founded by an initial group of countries, companies and intergovernmental organisations that are willing to actively contribute to the GFCE.

5. The GFCE aims to be a platform for the development of initiatives that could benefit parties beyond the GFCE membership. The GFCE is open to new members, provided they subscribe to the The Hague Declaration on the GFCE, accompanying the official launch of the Global Forum on Cyber Expertise. GFCE members will be consulted on requests for membership.

Structure and Functions

6. The structure and operations of the GFCE are based on four components:
   I. an inventory of current efforts undertaken in the field of cyber capacity and expertise building;
   II. an umbrella framework for the promotion of new initiatives, as well as enhancing and expanding existing ones;
   III. a platform for high level discussions;
   IV. an Administrative Unit.
I Inventory of current efforts of cyber capacity building

7. Through the GFCE an inventory of current efforts in the field of cyber capacity building will be made available and kept up to date. This overview will allow GFCE members to identify and fill gaps in existing bilateral, multilateral, multi-party, regional and international capacity building activities and coordinate their efforts and contribute to bridging the digital divide.

II Umbrella framework for Initiatives

8. GFCE-members take new concrete initiatives or enhance and expand existing ones to strengthen capacity in cyber, through sharing experiences and best practices or other in-kind assistance, funding for capacity building projects, or a combination thereof (hereinafter: “Initiatives”). The Initiatives focus on a specific cyber area where there is a need for assistance or sharing of expertise and taken under the umbrella of the GFCE by two or more GFCE members (hereinafter: “Initiators”). The Initiators formulate the needs and assistance that a particular Initiative will contain. In addition to government entities, intergovernmental organisations or companies offering their own expertise, civil society, think tanks, academia, and in some instances international organisations, that possess expertise in certain cyber areas, could also play a role in an Initiative when invited to do so by the initiators.

9. New Initiatives can have a geographic or thematic focus, or can have both. The preliminary focus areas identified for capacity and expertise building within the GFCE are:
   - Cybersecurity;
   - Cybercrime;
   - Data protection;
   - E-governance.

10. The focus areas will be evaluated on a yearly basis and may be amended by consensus of the members of the GFCE.

11. The setting up of an Initiative within the GFCE will generally consist of the following four phases. These phases should be seen as guidelines.

   Phase one: Set-up

   12. The Initiators take the lead in setting up an Initiative. Of these Initiators, at least one party has knowledge and/or expertise in one of the above-mentioned cyber areas, while at least one other party has a specific need for building up capacity in that particular field. Civil society may contribute by making suggestions for new initiatives.

   Phase two: Identification

   13. These Initiators formulate the specific assistance that is needed in the Initiative, and the means and ways of conveying the assistance or sharing the experience (so-called terms of reference). The assistance can be in the form of financial donations and/or in-kind expertise, for example sending experts to give trainings, or by sharing reports, best practices and lessons learned. Formulating the needs can either be done by the Initiators bilaterally or in a multi-party and multi-stakeholder
setting (i.e. a regional or thematic seminar). Civil society, the technical community, think tanks and academia can also be involved in the formulation of specific assistance at the discretion of the Initiators.

Phase three: Recruitment
14. The Initiators recruit participants for the Initiative amongst GFCE members. This gives other members of the GFCE the opportunity to either contribute to the Initiative (with financial means or with in-kind expertise) or to indicate that they need the same assistance in building capacity. The setting up and the coordination of the Initiative remains the responsibility of the original Initiators.

Phase four: Implementation
15. When a clear need for capacity building has been established and adequate (financial or in-kind) resources have been found, coordinated by the Initiators, the Initiative will start its implementation phase. It is at the discretion of the Initiators to involve civil society, think tanks and academia, or use expertise within regional organisations, as implementing partners within an Initiative. Non-GFCE members could benefit from the results of specific Initiatives taken by GFCE members by associating themselves with these initiatives.

16. The Initiators will disseminate the results, lessons learned and best practices of an Initiative amongst GFCE members upon its completion to maximize the effectiveness of other Initiatives.

III Platform for high level discussion
17. An annual high level meeting amongst members of the GFCE to evaluate progress made will take place, preferably in the margins of future Global Conferences on Cyberspace. The dialogue will provide the opportunity to discuss and (re)formulate requirements as well as best practices on cyber capacity building in the focus areas. The development of best practices will promote a continuous policy discussion about ways and means to respond to emerging challenges in the cyber domain, while preserving each member’s -internal decision making processes on implementation of specific measures. Civil society, the technical community, think tanks and academia will also be encouraged to be involved in the discussion, contributing to the development of best practices and advising on the formulation of requirements.

IV Administrative Unit
18. The Administrative Unit will, inter alia, provide the necessary administrative and logistical support to GFCE members. It will maintain an overview of ongoing Initiatives and circulate the results of Initiatives among the GFCE members. It will facilitate and manage the sharing of information by GFCE members and, as appropriate, other relevant stakeholders of their relevant national practices and programmes, documents, and information regarding Initiatives taken under the umbrella of the GFCE.

19. The Unit will support and assist with logistical planning for the annual high level policy meeting, preferably to be held in the margins of future Global Conferences on Cyberspace. It will, inter alia, assist in the production of an overview of results of the GFCE and its initiatives to present to the GFCE members.
20. The Netherlands will initially host and finance the Unit for a period of four years after the launch of the GFCE. Consistent with the informal format of the GFCE, there will be no assessed contributions from GFCE members to finance this Unit. The Unit is expected to include four persons and will seek to include, where possible, individuals from other GFCE members.

21. At the first annual high level policy meeting on cyber capacity and expertise building, preferably in the margins of the next Global Conference on Cyberspace, the structure and operation of the Unit will be assessed and reviewed. The most appropriate structure, operation, financing, and location of the Unit over the longer term will be seen in conjunction with the development of the GFCE and its long term requirements.