Department of Information Technology
Ministry of Communications and Information Technology
Government of India
Electronics Niketan, Lodhi Road
New Delhi – 110003

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 at the above address or on email id '**grai@mit.gov.in'**

Department Of Information Technology

National Cyber Security Policy

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

Contents

Annexure I - Stakeholder agencies

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 proviides an over view 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 time*

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 up gradation/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:

- **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 market place, 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

- 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 orgnisations' 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

- 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

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.

Annexure I

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.

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 competentance to provide quality assurance and conformity assessment services in IT

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.