Compilation of Comments
On
Discussion draft on National Cyber Security Policy (draft v1.0, 26-March-2011)

The comments received on Draft National Cyber Security Policy (draft v1.0, 26 March 2011) have been compiled on the basis of

I. Generic Comments

II. Clause wise specific comments. Under this, each Clause/ sub-clause of draft National Cyber Security policy (draft v1.0, 26 March 2011) is reproduced in italics followed by comments on that particular clause.

I Generic Comments

A. AKS Information Technology Services Private Ltd.

III. Setting up of a full-fledged IT System Testing Lab for sanitization and providing security assurance levels to the products/software, similar to Common Criteria Test Lab (CCTL)

IV. As already mentioned in the draft document, the critical infrastructure will be identified and classified. It is recommended that the security audits of infrastructure with higher criticality be mandatorily conducted on half-yearly basis.

V. Since the purpose of the proposed document is to ensure highest levels of cyber security, a mention may also be made of the punitive actions that may be instituted against unscrupulous, unethical and unprofessional agencies and individuals.

B. Ministry of External Affairs

1. We support the initiative taken by the Department of Information Technology to prepare a National Cyber Security Policy , which we hope will go a long way in creating a secure cyber space in India.
2. We in the Ministry of External Affairs have been sensitive to cyber security for some time and have taken lead in issues like organizing IT security training to officers and staff members of the Ministry. We have been emphasizing that whatever may be done at the level of service provider or the server level, security in the cyber space cannot be ensured unless the end-user is well aware of the pitfalls and takes all the necessary precautions, many of which are very basic and simple. This aspect may be highlighted in the proposed GOI policy.
3. MEA's own IT security policy deals with policy for general users, which includes access control, software update policy , antivirus/ firewall, internet usage, data protection and storage , removable media, user responsibility and penalty for policy violation. It also gives specific guidelines to IT Managers and IT security Managers. As the Ministry has Missions all over the world, the policy also gives guideline regarding hosting their websites and mail servers etc. In whole, it provides a complete package for all users in the Ministry.

C. IIT, Delhi

1. We may evaluate the proposed draft on national cyber security policy by considering its structure in terms of the following essential components of any comprehensive policy document.
2. Various essential components of a policy are enumerated below:-

   a. Background
   Social, economic, technological and political backgrounds should be considered in-depth while deciding on policy guidelines.

   b. Environment
   A developing country like India would, of necessity, be characterized differently than developed countries. Our present position on cyber security maturity continuum has to be factored in, while formulating a policy.

c. Scenario Building
The future trends in terms of various related issues need to be factored in.

d. Clear Objectives
Short and long term consistent and realistic objectives should be finalized

e. Priorities
In order to achieve the set objectives, the priorities are to be decided. A hierarchy of policy would help us identify deep drivers. We need to address fundamental root issues to be able to sustain secondary issues.

f. Feasibility
A very attractive policy statement will be of little value if it cannot be translated into an action plan.

g. Resources
The policy to be actionable should consider available resources and their budgeting to support the short and long term objectives.

h. Dynamic Nature
Policy should not be static in nature. It should be flexible so as to be tuned to the changing needs. There must be a constant review to improve the policy and modifications should be carried out from time to time to remove any impediments.

3. The cyber security at national level is a complex concept with various dimensions. Each dimension can be addressed by prioritizing most important objectives. Ongoing research for Indian context at Department of Management Studies (DMS), IIT Delhi has identified and prioritized the key issues under various dimensions of cyber security. The identified dimensions and issues under them can be readily mapped with the issues articulated in the draft policy. The structuring of objectives in component dimensions would enable better resource allocation and program development. The details can be shared if formally requested by DIT.

4. The scenario building in keeping with trends in technology could be incorporated considering challenges of 'Cloud Computing', wireless technologies and emerging 'Next Generation Networks'. We need to initiate programs as feasible with near and long term perspective.

5. The document seems to have more focus on 'Information Technology' aspects of cyber security and is prepared by Department of Information Technology. For any effort on national level to secure cyber space, protection and survivability of our telecommunication networks is extremely important. Without dependable telecommunication infrastructure in the face of natural or manmade disasters, our national security objectives would not be met. The proliferation of 2G/3G technologies in the mobile phones and inadequate attention to security issues can be a major challenge. It is recommended that a joint group of DIT and DOT (unless already in place) firms up the objectives for a comprehensive policy.

6. The draft policy is a welcome though belated activity. A comprehensive policy is prerequisite for the national strategy to secure cyber space. Time lines and measurement methodologies for the agreed action plan is very crucial. At DMS, IIT Delhi a research project has evolved a 'National Information Security Index (NISI)' construct for Indian context by using Delphi and AHP methodologies. The findings are based on judgment of expert participants from Indian industry, government and academic institutions. Its usability by DIT could be evaluated and this instrument could be used for monitoring progress of our national cyber security effort.

7. The document has flagged most of the important issues and by restructuring the material in terms of components as described in para 2 above, we may get clarity of vision while formulating the action plans.

D. Shri Ankit Mehta

1. If user is getting some frequent attacks from an IP then he/she should be allowed to log a complain against IP. (Implementation like dnsbl)

2. He/ she should allow to log complain against potential attacks from IP to ISP of attacker

E. **US India Business Council**

On behalf of the members of the Telecommunications Industry Association (TIA) and the U.S.-India Business Council (USIBC), we respectfully submit the following comments on the Department of Information Technology's *Discussion Draft on National Cyber Security Policy ("Discussion Draft").* As the U.S. industry conveners of the U.S.-India Information and Communications Technology (ICT) Dialogue, we greatly appreciate the opportunity to comment on the draft and hope that the following submission will prove useful as the Department finalizes the Government's cyber security policy.

We strongly support the strategic perspective outlined in the opening paragraphs of the paper. The recognition of the importance of the ICT sector to India's current and future growth and prosperity and the associated societal benefits are essential components which must be both kept in mind and preserved when developing a suitable cyber security ecosystem. We are equally appreciative of the recognition that our networked environment is global. Finally, we appreciate that all stakeholders have a role to play in the cyber security ecosystem. In fact, this is one of the principles of the Organisation of Economic Cooperation and Development (OECD) Guidelines on Security of Networks and Information Systems – each according to his role.

The Discussion Draft echoes many of the key principles of cyber security critical to the private sector:

- Recognizing the borderless, interconnected and global nature of today's business, information flows and cyber environment;
- Leveraging public-private partnerships, including existing initiatives and resource commitments;
- Responding rapidly to emerging threats and adapting to emerging technologies and other uses of information;
- Using flexible and risk-based policy and regulatory models;
- Enhancing education and raising public awareness; and
- Focusing on addressing and preventing harm.

As the draft policy emphasizes, creating an adaptive and flexible approach to cyber security requires robust public-private partnerships to enable vital information sharing and cooperation among public- and private-sector stakeholders. These partnerships are crucial to building capacity and developing best practices and procedures that will help government and industry stakeholders coordinate reactions and responses to existing and future threats.

We are pleased that the policy paper recognizes the need for international cooperation and would note that there are a number of important international organizations involved in cyber security, including the International Standards Organization, the Common Criteria Recognition Agreement, the IEEE, the International Telecommunications Union and the Organisation of Economic Cooperation and Development. Further engagement by the Government of India (GOI) with these organizations could be enormously helpful as the Department develops a more comprehensive cyber security strategy. In particular, the rise of cloud computing requires an international dialogue to harmonize the increasingly inconsistent web of rules that threatens to prevent data from flowing seamlessly across borders.

We understand that DIT plans to regularly update and refine this National Cyber Security Policy in line with technological trends and security challenges posed by such technology directions. We commend this approach. Efforts to improve cyber security must be adaptable to rapidly emerging threats, technologies, and business models. Because policy can quickly become obsolete in this environment, national strategies should be reviewed regularly to determine if they need refining or updating for technical or business reasons.

We also understand this National Cyber Security Policy creates a framework that will lead to specific actions and programs. We urge DIT and all other relevant GOI agencies involved in updating and implementing India's general Cyber Security Policy and/or accompanying actions and programs to use an open process, including public comment procedures and other methods of obtaining feedback from outside stakeholders.

We look forward to continuing our close collaboration to address shared security challenges. We believe that an open and full stakeholder consultation process is vital to ensuring policies that meet the security needs of both countries, while fostering continued growth and innovation in the ICT sector. Our associations and member companies stand ready to serve as full partners in this important undertaking.

F. KR Information Security Solutions

While the majority of the document gives specific recommendations and lays down concrete actions to be taken, there are certain areas which the appearance of an 'approach paper' look. For example, in Section 3.3, Security best practices - compliance and assurance under the sub-section 'E-Governance' it says that "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." These remarks should not appear in a Policy document which aims to lay down the exact requirements that must be met by organisations.

G. Data Security Council of India DSCI

At the outset DSCI would like to congratulate DIT for drafting a national cyber security policy which will enable secure computing environment and adequate trust and confidence in electronic transactions. The policy rightly points out the complete ecosystem by virtue of which a secure computing environment can be created in India. It takes into consideration the latest developments and discussions that are taking place internationally in the area of cyber security. The policy not only talks from a strategic perspective, but also touches the real threats which can impact the cyber security of the country. The policy demands enabling security processes which strengthen the security against evolving threats and vulnerabilities and create an early warning and response mechanism. The draft National Cyber Security Policy not only promotes best practices which provide assurance and compliance but also creates a sense of trust in electronic transactions. The requirement of legal framework for law enforcement and security information sharing and cooperation is also commendable. The policy touches the need for a strong R&D requirement and enabling people through security education and awareness, skills training and certification. DSCI is fully supportive of these steps and is willing to work with DIT through a Public-Private Partnership model, in the areas deemed fit by DIT.
The National cyber security policy has to identify the roles and responsibilities of the public and private sectors, since more and more infrastructure is owned and operated by the private sector. DIT has already identified infrastructures that are classified as Critical Information Infrastructure, namely Defence, Finance, Energy, Transportation and Telecommunications. The following analysis of some of these sectors shows that a significant part of the critical infrastructure is owned and operated by the private sector:

1. The telecom sector is mostly governed by the Private players, except MTNL, BSNL. The 'Global Under Sea Cable Communication Infrastructure' is largely owned by the private players.

2. The banking sector where more than 30% of the total transactions are done online and the value of these transactions is over 80% of total transaction value, has large number of foreign and private banks

3. Stock Exchanges – Major stock exchanges BSE and NSE are private players wherein most of the transactions are done through electronic medium

4. Airline industry is dominated by private players with Air India being the only the government enterprise

5. Energy & Utility – Though this sector is largely dominated by government players, the distribution is largely controlled by private partners

Thus, private sector is equally important when it comes to securing a nation's cyber space and it needs to be greatly involved in government's cyber security initiatives through various mechanisms including Public-Private Partnership. While CERT-In is doing an excellent job in the government sector, same needs to be replicated for the private sector through establishment of appropriate agencies within each of the identified private sectors, that co-ordinate with CERT-In and / or National Nodal Center that may be created. DSCI feels that in this policy, there should be a recommendation for establishment of National Nodal Center, which will co-ordinate the efforts of both the public and private sectors and will also assign roles and responsibilities.
DSCI has consulted its chapter community (1150+) and corporate members (568) and is pleased to submit the following comments on behalf of the industry:

A. There should be a National Command and Control Centre which should be responsible for coordinating cyber security related activities at the national level for both the public and private sectors.

B. Both the Private sector and the Public sector should coordinate within their respective verticals with respect to the following:

1. Security Alerts and Vulnerabilities impacting their ICT infrastructure
2. Tracking Botnet, Phishing sites, Spam, Malware, etc. and the steps to overcome these issues
3. Sharing of Best practices
4. Early watch and warning system
5. Incident response mechanism
6. Work with their respective counterparts nationally and internationally. For example, the Indian banking sector CERT should work closely with its counterpart internationally, much the same way as CERT-In does with the CERTs of other countries.

C. The national cyber security policy should create a platform that facilitates information sharing and analysis between public and private sectors on a continuous basis.

D. The policy should focus on creating awareness on preserving evidence for Cyber Forensics after a Cyber Attack has taken place. It should focus on Cyber Forensics capacity building in terms of infrastructure, expertise and availability of human resources.

E. There is a need to create enablers for Cyber crime tracking, cooperation for capacity building between industry, LEAs and Judiciary. The policy should enable this through Public-Private Partnership.

F. The policy should focus on creating ongoing cyber security education & awareness as no amount of education & awareness is enough and there is a continuous need for Public-Private Partnership in all sectors of the Indian economy.

G. The national cyber security policy should enable creation of an ecosystem that works globally to develop a legal regime for defining the 'rules of the road'. An example of such a rule could be on how to distinguish between a cyber warfare and cyber attack. This can be done on the lines of (similar to) EU cyber crime treaty or Hague or Geneva Convention or LOAC (Law of Armed Conflict).

H. There is a need to create a group having representation from the public and private sectors which develops and issues best practices based on international standards to protect Critical Information Infrastructure – (e.g. SCADA systems). The group can also act as an agency for information dissemination and information sharing. For example, such a group can spread the learning of Stuxnet attack in the industries that use SCADA systems.

I. As highlighted earlier, Information infrastructure including critical information infrastructure is largely owned and operated by the private sector, i.e., critical national security operations is in private industry's hands but security investments are largely driven by business plans. Regulations add cost and may not necessarily improve security. Government through this policy should create incentives for industry to invest in cyber security beyond what is necessitated already by corporate business plans.

J. The policy should enable the government to fund the private sector for conducting research in the area of cyber security.

K. The policy should promote use of strong encryption for secure business, government and military communication.

L. Adoption of Cloud Computing will increase significantly with time because of the economic benefits it offers. But in the use of Cloud Computing, the data (corporate secrets, IPRs, personal data, etc.) will transverse international boundaries as the servers hosting the Cloud services could be located anywhere in the world. In such a scenario, government should have appropriate policy in place, which is capable of addressing the cyber security risks arising from use of Cloud Computing (e.g. non-availability of data to LEAs as it is stored in a different jurisdiction).

M. The policy should address the risks arising from the widespread use of social networking as this medium is being increasingly misused by the criminals and terrorists.

N. Similarly, the cyber security policy should have provisions to address security risks arising from the use of new technologies and service delivery mechanisms.

O. Telecom security is one of the key pillars of cyber security. Thus, the cyber security policy should attempt to strengthen telecom security esp. through establishment of testing labs for telecom infrastructure (equipments, hardware).

P. The policy should suitably balance Security and Privacy esp. in case of National Security and at the time of cyber emergency / crisis.

Q. The policy should debate and discuss the concept of trusted identity versus anonymity on the internet. This is being currently debated internationally, esp. in the US.

H. **Deloitte Touch Tohmatsu India Private Limited**:

Creation / adoption of a Cyber Risk Governance Framework by organizations may be suggested as part of priorities of actions, e.g., Development of a snapshot of an agency's Cyber risk footprint to quickly identify and prioritize the riskiest elements in their Cyber footprint, including employee actions, policies and processes. Then managing the Cyber risk lifecycle including risk identification and evaluation, and control testing and remediation and as part of overall risk governance, managing the Cyber risk program, including policies and procedures evaluation and development, and package selection and implementation. For instance, there should be periodic review of cyber security policy by organizations depending upon nature of business changes in the business etc.

National Cyber Security Policy may also include Non-Profit organizations as any times they hold / possess sensitive information which can be critical to National Security.

Resolution of any activity which could result into cyber threat should happen by performing analysis by authorized and appropriate tools only.

Organizations procurement policies (specifically IT infrastructure) should have norms on Cyber security and Procurement process must evaluate key risks and impacts with focus on cyber risks.

Cyber Security parameters may be also enabled and defined for etoys i.e. ipad devices etc as public domain are used to carry a lot sensitive data.

I. Internet and Mobile Association of India

Introduction:

On behalf of our members we would like to commend the Government of India for approaching the issue of cyber security on the basis of international best practices and cooperation with the private sector. We sincerely hope that further developments in policy measures related to NISP would be done in consultation with open public consultations and would also take into view the private sector initiatives in this space. Finally, NISP should also be based on two-way flow of information and dara sharing – private to government as well as government to private.

In this submission we are also assuming that issues such as Encryption and Escrow are not directly a part of this paper.

Here is our detailed feedback.

General Observations:

1 NISP requires being very flexible, responsive to ever-changing cyberspace and should have longer shelf life. It should therefore be kept opne for wider interpretation and be able to cut out dogmatism.

2 As a nation we need to much more actively involved in Internet governance rather, than control. This has been a weak area. As we are not active in Internet Governance bodies, this takes away our strategic depth and effective handling of issues with complete in-depth understanding. Thus guidance in NISP, where as nation we need to be proactive in Internet governance bodies may be necessary.

3 There is need to clearly state that NIB from time to time will declare as to what activities or actions in Indian Cyberspace would amount to aggression on India and if such parameters are crossed then we may retaliate diplomatically or mount counter offensive in Cyberspace against state as well as non-state actors.

4 Though there has been repeated mention of R&D but specific involvement and integration of 'Academia' in furthering the national cause of Cyber Security education may be necessary. This may include development of curricula, capacity building and hub of new ideas. Student exchange programme with other countries and publication of research papers at various universities level may be in the interest of our country. This may find mention in the NISP.

5 Our pro-active participation in developing standards (national as well as international) requires specific and clear mention. The STQC may be given similar charter as NIST of the US at least in the field of Cyber Security.

6 Though the "role and responsibilities" of private persons and bodies have been mentioned but same is kept hazy for government department. There is lack of clarity in charter. It may please be noted that overlaps especially in respect of surveillance of critical Information Infrastructure of enemy /probable enemy state can be jeopardised by the weakest link in the chain, and if there is any lack of coordination a major operation may collapse. Therefore tasking of surveillance and cyber –intelligence outside the country must be positively controlled by NIB and should be stated so unambiguously.

7 National policy on joining / creating international treaties / fora for joint cyber crime operation must be spelt out in NISP.

8 NISP must state the nodal point of interaction in case of any cooperation with foreign entity for Cyber Crime investigation.

9 Please read through draft ISO 27037 on International standardisation for capacity building for "First Responder" for gathering Cyber Evidences which can be admissible in courts of other countries. It will be necessary to align our procedures and practices so as to accept the Cyber evidences gathered in accordance with ISO 27037 in third nation. (This should be a MUST clause in NISP).

10 National policy must include the mechanism and methods for farming rules for Cyber crime in a transparent and consultative manner.

11 NISP is silent on privacy issue. The links with various existing laws in place should be drawn out explicitly.

12 There is no mention of abuse / misuse of power from information gathered for national security purposes by government officials/agencies. NISP must make clear and make an unambiguous policy statement as to how such cases should be treated. This will help preventing Human Rights violations as well as corruption.

13 Though TRAI planning to look into governance issues of Cloud Computing. This facet may require appropriate mention in the NISP after a due consultative process by stakeholders.

14 After introducing appropriate amendments, it may be prudent to go for last and final public inputs on such amendments prior to submitting it to CCS for clearance and publication.

J. **Microsoft Corporation (India) Private Limited**

Microsoft thanks you for your commitment to and leadership on cyber security and critical information infrastructure protection. The ***Discussion Draft on National Cyber Security Policy*** demonstrates an understanding of the security challenges facing the cyber ecosystem, and provides a necessary strategic context and approach for the Government of India to help address those challenges.

First and foremost, we support the inclusiveness of the policy as well as the consultative approach being undertaken to develop it. The Internet has fundamentally transformed how we communicate and interact as individuals, businesses, and governments. As such, the policy appropriately provides a framework to improve cyber security for the "whole spectrum of ICT users and providers."

We also strongly endorse the focus on partnership and collaboration. The Internet is a global, borderless, shared and integrated domain making such partnership and collaboration a necessity, both domestically and internationally. And unlike other domains, cyberspace cannot be secured by the government alone; it requires a coordinated effort involving the owners, operators, and vendors that make cyberspace possible.

In response to your request for feedback, we offer the following three high level themes for your consideration as the discussion draft continues to evolve. We have also provided more specific comments and recommendations by section as an attachment.

Risk management and compliance –Risk management and risk management principles and practices can be found throughout the discussion draft, and are described, although not directly named, in bullet five of the key policy considerations. We believe that risk management is the only feasible approach to cyber security, and therefore, consider this a foundational element for the approach presented in the document. Neither governments nor industry have unlimited resources, and using risk management will focus deployment of the available resources where they will be most effective. While clearly founded on risk management, we recommend that the language regarding security management in critical infrastructures be reviewed and updated to better align with those principles.[1]

[1] For example, phrases such as "reduce vulnerabilities" should instead focus on "reduce risk" as vulnerabilities are only one of three factors of risk (the other two being consequence and threat) that should be considered. The concepts of strategic and operational risk management spanning efforts to prevent, protect, respond, and recover could also be better integrated. Proposed revisions for consideration are included in the attachment of specific comments.

We also strongly endorse the approach of developing and documenting "information security plans" and "implementing controls consistent with international standards" to reduce overall risk, as called for during the discussion of security practices for government and critical sectors. We believe that a baseline of security policy and controls, based on international standards, applied broadly and consistently, across government will improve collective security most efficiently and effectively at scale. Such a common baseline requirement for all ministries, departments at the central, state and local government levels will have the most immediate, broadest, and sustained impact. Some ministries and departments may then apply additional practices that exceed the baseline to address

their own unique risks. The application of such security policy and controls in critical infrastructures, however, needs to be further explored as it is not yet clear from the document what comprises critical infrastructure nor what the full implications of that designation are. Finally, we support the need to verify that certain established policies and controls have been implemented, yet the language in the draft document regarding compliance is somewhat unclear - who would do the risk assessments, periodic evaluations, and audit? We believe that international standards and existing certification regimes, such as the International Organization for Standardization 27000 series, should be the primary mechanisms to verify compliance with security requirements.

Infrastructure Assurance and Lifecycle Management –We strongly support the position that "security needs to be built-in" at the earliest stages. Microsoft's Security Development Lifecycle is the industry-leading software security assurance process that combines a holistic and practical approach to introduce security and privacy throughout all phases of the development process, and has proven to be effective at demonstrably reducing vulnerabilities.

Just having security built-in, however, will not suffice; security must also be maintained on an ongoing basis until systems are retired. The information infrastructure is constantly evolving as new systems, elements, and innovations are added, removed, and replaced; the threats facing that infrastructure are also both constantly evolving and growing in number and sophistication. This dynamic environment similarly requires dynamic management. We encourage the Indian Government to consider how to enhance the confidence in and security and integrity of systems across their full lifecycle - from design and development, to installation and removal.

Indigenous innovation - Microsoft is fully supportive of the Indian Government's efforts to encourage indigenous capacity and the growth of domestic ICT suppliers. We believe a vibrant ecosystem of software and service providers helps to meet local needs and enables participation in the global marketplace. Since entering India in 1990, we have worked closely with the Indian Government, IT industry, academia, and local developer community to support and grow the local IT industry through our partner enablement programs. The discussion draft, however, seems to imply that indigenous innovation will automatically produce more trustworthy or secure products and services. We anticipate the experts in DIT can appreciate that this is an erroneous and flawed presumption. A thriving indigenous ICT industry will definitely benefit India's economy; it will not necessarily produce more secure products and services.

We encourage the Indian Government to develop a policy that provides access to best of breed products and services and at the same time exposes the Indian software industry to the global marketplace. Trusted vendors and secure products are important and valid concerns, and as such, we believe that policy should be technology neutral and focus on enabling a market that drives trust and security into products and services. It should focus on how products and services are produced, instead of where, and be founded on risk management, international standards, and transparent practices.

Microsoft thanks you for your continued efforts to improve India's cyber security posture. Developing a national cyber security policy is a major undertaking and we appreciate the opportunity to engage with you on this effort. We look forward to continuing to work with you to evolve the policy.

K. **Government of Andhra Pradesh, IT&C Department, Infrastructure Wing**

1. Identification of Critical Sectors of the economy and establishment of Sector specific cyber security Standards may be necessary.

2. Cyber Security Standards for different aspects of the cyber space such as Network, Computers, & Data may be established

3. Cyber security standards compliance / enforcement mechanism may be defined for Critical sectors.

4. Co- ordination process with already available compliance / enforcement mechanism may be defined

5. Minimum Budgetary support for enforcement of Cyber Security in the Critical sectors may be recommended (e.g. US number 0.3 % of the total budget)

6. Policy may extend the scope of applicability of the policy to Indian Government missions abroad and Indian Public sector organizations' offices abroad

7. Policy may recommend Data Quality guidelines for Government information made available through portals, Department Websites etc.

L. **Department of Telecommunications (Unit: Security)**

The draft cyber security policy seems to cover all the important aspects relating to cyber security. However, the following suggestions are tendered:

i. It may be appropriate if 'Guiding Principles' for the policy and the 'Objective' of the policies are included and stated almost in the beginning of the policy. The 'Guiding Principle' will help in keeping the policy focused, and making sure that the policy is within those principles. The 'Objectives' will help in re-checking whether anything is left in the policy for achieving those objectives.
ii. Draft policy something seems to be too verbose. Hence, an attempt can be made to remove the redundant words and duplications.

M. **Software Freedom Law Center**

Executive Summary

The policy in its current state is a crucial first step towards creation of a suitable cyber security ecosystem in the country. However, the policy must take into account the following considerations in order to devise a comprehensive approach and strategy for protection of Cyber space in India.

1. Detailed study and description of the threat landscape should be carried out in line with the approach followed by other countries;

2. The focus of the policy should be on critical infrastructure;

3. Software running critical services and infrastructure should be audit-able and verifiable by the Government and capable of "designing in" requisite security measures; Cyber Security requires verifiable software engineering practices and thus the policy should mandate them; Crucial nature of the mobile network governance should be considered and made a part of a comprehensive policy;

4. Open Standards compliance should be a necessary component of a comprehensive national Cyber security policy;

5. The Policy should determine the role the government should play in the defence of critical infrastructures, while safeguarding privacy and civil liberties;

6. The Policy should talk about creating an information and threat-sharing plan with private industry that protects trade secrets; develop a centralized process — perhaps through a non-profit organization — for communicating known threats to industry and government agencies;

7. The Government should support research and development of technologies to enhance security; provide the research community with event data to help them create tools and testing models for securing networks.

The detailed Analysis is quite exhaustive. The comments pertaining to the various clauses and subclasses have been covered under the clause wise comments. However the detailed comments submitted by Software Freedom Law Center may be referred at "Annexure-A".

N. **ITD J&K**

Considering our knowledge and experience in the Cyber Security domain, we have few suggestions listed below which may be considered for the said policy document:

1. A recommended ACL Guidelines (File System, Network, Database, etc) may be included.
2. Considering the augmented use of Wireless media, use of secure protocols like RADIUS, EAP, WPA, etc and superior encryption techniques for better security, may be included.
3. Use of IDS/WIDS & IPS/WIPS or better technologies may be recommended for enhanced security.
4. There may be provision/ recommendation towards System Administration (onsite/ remote) to check permissions (for installation of tools/ software) in POPs and APs. A tool may be recommended for the same.

O. **FICCI**

We feel that the draft National Cyber security policy is an exhaustive policy statement that lists a number of new initiatives that the Government, the industry and public at large will need to take to bring about a comprehensive cyber security climate in the country. It aims to enable this through a number of public private partnership initiatives. It is a forward looking policy statement and captures most of the critical issues that impact the cyber space today.

The policy aims to create a cyber security framework. This framework would enable the Government to follow it up with a number of specific actions and programs to enhance the security posture of the country's cyber space over a long period of time. These programs while addressing the security threats will also enforce added responsibility on all citizens, service providers, Corporate and Government bodies. It will also provide lot of new opportunities to companies engaged in the security business.

The policy proposes some significant measures that will greatly enhance the cyber security posture of the country as also provide a number of opportunities for the private sector to partner with the Government. Notable among these are in the setting up of a country wide secure Intranet to connect critical infrastructure, National cyber alert system, Sectoral CERTs and others.

Cyber security Principles

We feel following guidelines will help in building and implement comprehensive and workable cyber security policy that functions at the national and global levels.

1. **Trust**—cyber security policy should enhance the confidence of consumers, businesses and governments in the confidentiality, integrity and availability of the online environment.
2. **Innovation**—cyber security is a fast-paced race, in which we must stay ahead of cybercriminals who adapt constantly. Cyber security policy should maximize the ability of organizations to develop and adopt the widest possible choice of cutting edge cyber security solutions.
3. **A risk-based approach**—consumers, businesses and government agencies seek to protect a wide spectrum of targets against a wide variety of cyber threats. Cyber security policy should enable them to implement the security measures that are most appropriate to mitigating the specific risks they face.
4. **International standards**—industry-led, internationally accepted standards to underpin the global information technology (IT) ecosystem and spur the development and use of innovative and secure technologies. Cyber security policy should preserve the role of international standards.
5. **Global policy convergence**—cyber security policy must recognize the borderless nature of the Internet, of the global economy and of cyber threats. As a result, governments should cooperate to ensure their national cyber security policy frameworks integrate with global approaches and practices

Opportunities for IT Industry

Promotion of open standards will result in development of indigenous IT infrastructure products.

Government aims to encourage wider use of PKI. This will result in demand for PKI enabling products and solutions in the identity and trust management space.

Organizations will need to get ISMS certification, IS System Audits, Penetration testing / Vulnerability assessment and enable data protection. This will require Government approved / empanelled vendors. Empanelment will achieve importance.

IT Security product evaluation and certification within the country is proposed. This will provide a new line of business around security testing around Common Criteria standards.

Government Secure Intranet Network - a country wide network is proposed. This will require setting up this network with possibly lot of indigenous components, manned and operated by Indian Companies.

Compliance Mandates will lead to big demand for periodic services around GRC, audit and IT assurance services.

P. **Infosys Technologies Limited**

We are of the opinion that the National Cyber Security Policy is a commendable and critical step towards consolidating the government's approach to establish a comprehensive cyber security strategy for India. Amongst others, the proposal to establish a national level nodal nodal agency on cyber security under CERT-In and sectoral CERT-ins for critical sectors is a welcome step towards effective implementation of the policy guidelines. This note addresses certain areas that may be re-aligned for better implementation of its objectives.

Implementation Period

The policy accurately identifies the risks being posed to the country's cyber space as imminent and therefore it is the need of the hour to prepare against such threats. In order for the policy to be implemented in a timely and effective manner, it may be a good idea to set out the timelines by which each of the phases enumerated in the policy are sought to be completed.

Q. Safenet Inc

I am of the view that as part of the organization structure India needs to have its own groups that are dedicated to

a. Study, Evaluation and Mandating security practices/standards that shall be binding on the requisite stake-holders. There shall be no ambiguity on what we seek to follow in the matters of National Security
b. Ethical Hacking/Auditors – To be used for the purpose of actively assessing the readiness of what different departments say they are ready against
c. Cyber Attackers - we can't expect to prevent something that we can't perpetrate on our own. Having the capability to launch a cyber attack of our own is an essential capability that India must possess

As daunting a task as it is, getting to a National Level Policy is a herculean task, and while every part of this document is thought provoking and I tend to think that it serves its purpose very well as it seeks to spur a debate amongst the respective stakeholders, it does need to evolve into a Timeline based action plan. Having said that, would you help understanding as to what are the next steps to getting this draft to execution?

R. United States Department of State

The Government of United States sincerely appreciates the opportunity to provide comment on the Department of Information Technology's discussion draft on National Cyber Security Policy. The

document addresses cyber issues of both national and international importance and we congratulate India for taking this important step toward strengthening its national cyber security. We believe that our bilateral conversation on cyber matters is one of the most important international relationships on these issues and the sharing of this document is evidence of this fact. We look forward to continuing this dialogue. To facilitate further discussion, the U.S. Government has these few recommendations on the draft strategy. We look forward to our continued collaboration on these important issues.

1. **The importance of implementation plans for cyber policy strategies.** In our experience, when clear leadership roles and responsibilities are defined at the start, it becomes much easier and more efficient to implement government-wide cyber security guidelines. For the United States Government, each Department and Agency designates specific groups or offices within their structure to maintain and implement cyber security policies through the coordination of the White House. Without a clear and defined structure, implementation becomes difficult and could result in duplication or gaps in important security responsibilities. We encourage the development of a more specific implementation framework that includes oversight and forcing mechanisms.

2. **Domestic capacity building:** India should consider establishing a training model for police, prosecutors and the judiciary on cyber crime based on international best practices. We recommend that other areas of domestic capacity building, such as building citizen awareness about the importance of good cyber security, be highlighted and differentiated from the needs of government workers and other private sector professionals. In addition, India should assess cyber security professional requirements in terms of quantity and quality before establishing a training program.

3. **The role of CERTs:** This policy document should highlight the need for continued cooperation with CERT teams around the world and participation in the Forum of Incident Response and Security Teams. We look forward to the forthcoming US-India CERT-CERT agreement. In addition, the document should address how to improve existing domestic channels for information exchange between Indian industry, law enforcement and the CERT community.

The United States and India enjoy a strong and growing relationship on cyber matters and the U.S. looks forward to continued dialogue and cooperation. The US and India have held several exchanges in the past on these matters and we would be eager to continue with consultations in order to expand upon the cooperative efforts already undertaken. The United States Government looks forward to future expert to expert dialogues, executive level exchanges and working level engagements on these issues and appreciates the opportunity to comment on the draft policy. This National Cyber Security Policy is a great step forward for India and the U.S. sincerely appreciates the opportunity to review and comment on this important document.

S. Ministry of Commerce, Trade Policy Division

This Department has no comments to offer. However, it is informed that in the Copyright Act, two new sections are being inserted namely 65-A and 65-B, Section 65-A deals with penal clause on any person who circumvents an effective technological measure with an intention of infringing rights. Section 65-B provides for protection of Rights Management Information.

T. BSA GLOBAL CYBERSECURITY FRAMEWORK

On behalf of BSA, its member companies and the international software industry, we congratulate the Department of IT, Government of India in developing the draft paper in National Cyber security framework for India, a much needed and essential public policy tool as India takes its place as the second fastest growing economy in the world.

BSA specifically supports the proposed framework's inclusion and emphasis on:

- A risk-based approach to cyber security
- Partnerships between government and industry

- International standards and best practices
- Innovation

We also strongly support the draft national policy's recognition that the use of legal software contributes to securing information and information system. BSA would be happy to offer training to small and medium enterprises (SMEs) on the benefits of sound ISO-aligned Software Asset Management (SAM) practices. Such practices offer them protection from security risks arising from the use of pirated software, thereby enhancing their competitiveness. BSA has already run SME training programs on SAM in partnership with the State Government of Karnataka, State Government of Maharashtra and The State Government of Andhra Pradesh. BSA has also had the privilege of running two workshops with the honorable Department of E-Governance within the Department of IT, Government of India on methods of implementing a sound SAM policy.

However, we believe that government agencies and large corporate, and not just SMEs, should also take advantage of comprehensive software management training and solutions to increase the stability and security of their IT system.

I would also like to draw your attention to the appended Global Cyber Security framework developed by BSA which we have engaged several governments around the world with and we would like to humbly recommended that the honorable Department also peruse through it and borrow from some global best practices as is seen fit during the finalization of this policy. The BSA Global Cyber security Framework may be referred at **Annexure-B.**

U. Ministry of Railways (Railway Board)

Assessment and certification of compliance: CERT-In has empanelled third party agencies for IT Security Assessment Services. These organizations may be categorized based on their expertise in specific domains such as Application Security, Network Security, or Services pertaining to ISO 27001certification. It is also suggested that a scoring system on the capabilities of the agencies should be introduced for easier selection of an appropriate agency from the panel.

Provision of Central Repository for all Security related information: A web-based repository of information may be generated and maintained, to which member organizations can upload as well as download information. This will help in information sharing among Sectoral Certs, Academic institutions, Private organizations and CERT-In.

V. Ministry of Mines

The following were the suggestions to be included for successful implementation of the policy:

1. Empanelment of consultants/agencies to facilitate Govt. Organization to identify security concerns, to formulate and implement cyber security as per the need of the organization.

2. Organization of regular orientation/training programmes for better understanding of cyber issues/vulnerabilities.

W. Chandigarh Administration U.T

The National cyber Security Policy is a great initiative in the country and the current drafts does address most of the challenges of the cyber space. However attention is drawn towards following issues which need to be addressed in the current draft policies :

- The current draft does not define Cyber Crime and Cyber Terrorism. In the current scenario it is imperative to distinguish the two terms and state clear definitions as in case of other countries such as U.S.

- When there is a cyber conflict, will "an internet shutdown" be a solution? What is the country's preparedness in this regard and how do current policies address such a major cyber threat/war scenario?

- How a nation's network topology indicates its resiliency to cyber attacks and to which extent and how is it addressed in the current policies?

- Social networks are playing an increasingly vital role in cyber intelligence, cyber counterintelligence, and cyber information operation. The current riots in London and Egypt are true examples to illustrate the roles of social media in wide spreading the internal unrest. It is important to consider as to how to properly control social networks in the interest of the nation?

- How to attribute or trace cyber attacks especially originating from international borders? In most of the cases pertaining to cyber attacks originating from outside countries available in media, no or substantial evidence has not been found to prove the source of attacks. This is even critical when the technology today permits attacks to be deflected or made anonymous. Network forensics is thus very crucial and the current policies must ensure that international cooperation also deals with aiding nations with cyber forensics.

- How to achieve assurance or confidence in the supply chain of software and hardware? As a consequence the stakeholder agencies Annexed As annexure-I in the current draft should avoid adopting foreign OS, foreign antivirus solutions and Chinese hardware for critical infrastructures especially the one which have not be tested.

- India currently has no means to control the malware entering through the Internet Exchange Points and also have no policies to regulate the malware and the content at such exchange points. This may also be indicated under the actions to be taken by user communities.

- Precise identification of critical sectors and infrastructure needs to be included as the Cyber Security Policies must ensure their security in a comprehensive manner which also requires that all hardware and software in such sectors are from sources. Promoting own private industry through strategic government intervention and promotion of policies which will promote indigenous industry is also the need of the hour.

- Considering the advent of virtualized services as a new paradigm of if IT service delivery, the draft policies must also ensure that Service Providers such as Cloud Service Providers should notify the subscribers if the cloud's security is breached and sensitive information is lost or exposed in a manner that creates a risk of identify theft. This can be attained by issuing data breach notification legislation as already present in the laws of other countries such as US and other European countries. It will be important to safeguard the privacy of data under the nation's legislation.

.

X. Information Technology Department Civil Secretariat, Srinagar/Jammu

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 and over view of what it takes to effectively protect information, information system & 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 ling period. The framework will lead to specific actions and programs to enhance the security posture of country's cyber space.

Observation:

A draft of the much needed National Cyber Security Policy has finally been released by the Ministry of IT / CERT-In, for public comments.

Key notable points:

- Creation of a national level nodal agency on cyber security under CERT-In and sectorial CERT-Ins for key sectors
- A national cyber alert system for early warning and response
- Local incident response teams at key locations, to liaison with expert teams with CERT-In for resolution.
- Creation of a Chief Info-security Officer post in all government and key sectoral organizations
- Open standards to be encouraged and a govt-private sector consortium to be created to promote these
- School/ college training program on cyber security to be instituted.

Analysis:

1. The policy should address privacy issues over use of shared / collected data.
2. The Cyber Security Policy doesn't prioritize. The policy indicates over 10 major initiatives without any priorities or timelines.
3. With many different stakeholders involved policy implementation, Interco-ordination between stakeholders should be clearly defined with proper checks and balances between them.

Y. <u>Information Technology Department, Government of Meghalaya</u>

The draft Policy document has adequately addressed all issues related to Cyber Space and its security. Cyber Security is always in continuum and newer proactive or defensive mechanisms have to be initiated to stay ahead of its perpetrators.

Further, the document also states about creation of certain organizations at National, Sectoral and local levels. It is recommended that states may also be required to have an institutionalized mechanism in place in order to ensure seamless sharing of information amongst these proposed agencies so as to ensure quickest and befitting response to any acts of vandalism in our National Cyber Space.

Z. <u>Information Technology Department, Government of Assam</u>

1. In government offices, there should be a policy for Internet access which shall clearly define the various access rules for different level of employee and different time restrictions. For example, during office hours some non-productive sites may be given restricted access.

2. IP usage policy should be enforced. Every employee (whose system is connected to the network) should sign the approved IP usage policy.

3. Government must enforce the rule that no one can host any official website without getting it security audited.

4. The Draft does not explain much about the physical security aspect and the manpower security aspect. It relies heavily on CERT-In and DIT being the nodal agency for security related matters but does not explain the benefit of having physical security and personnel security in place.

5. The Draft does not mention much about risk assessment and risk treatment for setting up an ISMS in a government organization. Risk treatment techniques are an integral part of an ISMS. Moreover the draft does not mention about adherence to ISO27001 procedures.

6. The draft also does not mention about intrusion detection techniques and intrusion prevention techniques. (IDSs and IPSs).

7. The draft is more generic in nature and might require fine tuning as far as the technical aspects are concerned to be universally acceptable.

II Clause wise specific comments

Clause 1.0 Security of Cyber Space – Strategic perspective

Comments on Clause 1.0:

A. Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's

Our Generic comments as summary of our response to all the below paras contained in the Draft policy

We also appreciate the strategic perspective outlined in the opening paragraphs of the paper. We are with the Government on the recognition of the importance of the ICT sector to India's current and future growth and consider that the associated societal benefits are essential components for developing a suitable cyber security ecosystem. We are equally appreciative of the recognition of the need to be "in tune" with the globally networked environment.

The Discussion Draft echoes key principles of cyber security critical to the private sector namely:

- Recognizing the borderless, interconnected and global nature of today's business, information flows and cyber environment;
- Ensuring for the rapid response to emerging threats and adapting to emerging technologies and other uses of information;
- Using flexible and risk-based policy
- Enhancing awareness
- Focusing on addressing and preventing loss

For creating an adaptive and flexible approach to cyber security and building capacity and developing best practices are vital for government and industry stakeholders coordinate reactions and responses to existing and future threats.

We commend the approach and efforts of the Government to improve cyber security and the thought that the same must be adaptable to rapidly emerging threats, technologies, and business models.

We suggest that DIT and all other relevant GOI agencies to use an open process, including public comment procedures and other methods of obtaining feedback from outside stakeholders.

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, and public distribution systems), Healthcare (telemedicine, remote consultation, and 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.

Comments on subclause1.1:

A. **Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's**

We appreciate the Government view that the IT sector has become one of the most significant growth catalysts for the Indian economy. Simultaneously it is important that those at the bottom of the Pyramid are also served with strong e-governance in important social schemes enabled by ICT.

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.

Comments on subclause1.2:

A. Internet and Mobile Association of India

Security measures proposed to be mandated under this policy should have direct relation to the electronic information / transaction proposed to be secured. Further all such security measures should be reasonable and commercially viable proposition.

B. **Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's**

In light of the growth of IT sector in the country, rapid social transformation & inclusive, 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.

C. **Department of Telecommunications (Unit: Security)**

Section 1.2 and 2.1 probably can be put together and need for action may be brought out more clearly.

D. **FICCI**

We whole-heartedly agree with this draft policy that the right kind of focus in creating a robust cyber security eco-system in the country, in tune with globally-networked environment, is the urgent need of the hour. The Govt., the Industry and all the stakeholders should co-operate and collaborate on a war-footing to attain this objective.

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 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.

Comments on subclause1.3:

A. AKS Information Technology Services Private Ltd.

For
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.

Should be
This policy caters for the whole spectrum of ICT users and providers, including home users and small, medium and large enterprises and Government & non-Government entities.

B. KR Information Security Solutions

The impression one gets from the heading of this section is that it describes who this policy addresses. However, on reading the actual contents, this does not become apparent. Rather this section describes what this policy is about.

Additionally, this section also states that this Policy is an evolving document, changing with the technological trends and threat landscape. This implies that there will be amendments/corrections/additions to this policy every time a new technology is adopted or a new threat emerges. This should not be the case. Policy documents are high level documents giving the intent of the Government on the issue. These documents should be technology proof and should change only if there is dramatic and sudden change in the environment it addresses. Policy documents should ideally list out what needs to be done and leave the "how" it needs to be done to the stakeholders.

C. STQC

Indicates that "the policy caters to a spectrum of ICT users and providers including small and home users, medium and large enterprises and Government and Non- Government entities" Whereas in the policy documents reference is made primarily to critical information infrastructure and Government organizations.

D. US India Business Council

Comment: Section 1.3 correctly notes that cyber security is an evolving issue and that government must be prepared to update and refine its policies to adapt to new technology and security challenges.

Recommendation: Given the evolving nature of threats and advances in technology, governments need to work closely with non-governmental stakeholders, including the private sector and other technology innovators. The need for open and consultative processes is essential to assuring that cyber security policies achieve their objectives in a way that fosters continued growth and innovation and strengthens the legitimate use of ICT technology by business, government, and individuals. To that end, we recommend the Government consider the formation of a public-private advisory board or consultation group mandated to provide advice on evolving threats, known vulnerabilities and opportunities in the cyber security space. Such a body would be chaired by the Government of India and its membership would be determined on the basis of criteria that do not discriminate against foreign companies or companies with foreign parentage. In such a public-private partnership, the private sector has an incentive to protect its assets for business reasons but also out of good corporate citizenship. The government often possesses threat information that can assist the private sector in protecting those critical assets. In a partner relationship, that information can be shared and then the private sector can make the investment to protect the infrastructure that is critical to the public good. Working within the construct of a public-private partnership, the private sector and the government can develop methodologies, assess risk and develop strategies to mitigate that risk.

In the United States, for example, the U.S. Department of Homeland Security (DHS) has two major responsibilities regarding cyber security: (1) coordinating U.S. government network security and (2) facilitating coordination of nationwide critical ICT infrastructure protection. The Federal Communications Commission (FCC) has also established a public private partnership to provide a forum for exchange of best practices on improving the security, reliability, and interoperability of communications systems.

Upon its establishment, DHS was charged by the U.S. Congress to draft a National Infrastructure Protection Plan (NIPP) to secure U.S. critical infrastructure. The plan identified 18 sectors critical to the U.S. economy, which included communications and IT infrastructure. The NIPP created the Critical Infrastructure Partnership Advisory Council (CIPAC) that provides a legal collaboration framework for the existing public-private partnership, where the private sector leads sector coordinating councils and the government runs corresponding government coordinating councils for the corresponding infrastructure sectors. As a result, in the ICT sector, there is both a privately run Communications Sector Coordinating Council and an Information Technology Sector Coordinating Council. In order to provide a level of confidentiality and promote exchange of information, the Congress included provisions to permit DHS to exempt the public-private approach to infrastructure protection (CIPAC) from certain laws requiring that government and private sector advisory council meetings be open to the public.

The Information Technology Sector Coordination Council (IT SCC) is currently comprised of 85 private-sector organizations representing a diverse array of information technology companies. The primary mission of the IT SCC is to bring together companies, associations, and other key IT sector participants to discuss sector security issues and engage with the public and private sectors in all areas of critical infrastructure protection. The IT SCC identifies sector critical infrastructure protection policy engagement topic areas and serves as the focal point for Critical Infrastructure Protection (CIP) policy strategy collaboration within the sector, with other sectors, and across all government levels. It facilitates information sharing among the IT sector, government entities, sector members, and other industry sectors and reviews and comments on CIP-related plans and policies. The IT SCC coordinates between and among the sector's policy-focused and operations-focused mechanisms and their government counterparts with regard to development of sector recommendations for preparedness and incident response and recovery plans based on the experience of members of the sector. The IT SCC develops sound practices and lessons learned, identify vulnerabilities and interdependencies, conducts risk assessments, and develops risk management strategies (including vulnerability remediation and policy enforcement) with respect to CIP. (For more information, please see: http://www.itscc.org/index.php)

E. Deloitte Touch Tohmatsu India Private Limited.

The statement "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 of India/country." Can be quoted in a more specific manner addressing the geography (India).

Section 1.3

a. No information on 'ICT' or any reference whatsoever

F. **Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's**

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. The framework will lead to specific actions and programs to enhance the security posture of country's cyber space.

Given the evolving nature of threats and advances in technology, governments can only effectively adapt by working closely with non-governmental stakeholders, including the private sector and other technology innovators to develop methodologies and assess risk and develop strategies to mitigate that risk.

G. **FICCI**

Target audience for Cyber security policy should involve all key stakeholders of India, specifically our rural hinterlands. Cyber space traffic in years to come will be dominated by users holding hand held mobile devices, so key policy considerations will have to also involve those very aspects rather than the conventional anti-virus & firewall method of security.

This section correctly notes that cyber-security is an evolving issue and that government must be prepared to update and refine its policies to adapt to new technology and security challenges. Because of the continuously evolving threats in the Cyber security space, it will be useful if the Government considers the formation of a public-private advisory board or consultation group mandated to provide advice on evolving threats and opportunities in the cyber security space. This board may be headed by the Government of India. The government often possesses threat information that can assist the private sector in protecting the critical assets. In a partnership relationship, that information can be shared and the private sector makes the investment to protect the infrastructure that is critical to the public good.

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.*

Comments on subclause1.4:

A. AKS Information Technology Services Private Ltd.

For
It needs to be dynamic in nature and have necessary depth to detect, stop and prevent attacks.
Should be
It needs to be dynamic in nature and have necessary depth to prevent, detect and stop attacks.

B. KR Information Security Solutions

One of the Considerations states that effective cyber intelligence is essential for a proactive defense and possible counter-measures. This would imply that any authority or individual can launch counter attacks. This would surely not be the case and hence this section needs to be worded carefully to attribute counter-attacks only to the authorized agencies

C. US India Business Council

Comment: This section provides information on the policy issues the GOI is considering in developing a national cyber security policy and strategy. Because this section will provide a foundational element for developing policy, we offer several suggestions to help clarify these important areas for consideration.

Recommendations:

- The third bullet in this section describes "cyber security intelligence" as an integral component of the security of cyberspace. While we agree with the intent of the statement—anticipate attacks, adopt suitable countermeasures and attribute the attacks for possible counter action—we suggest using the industry term of "situational awareness" rather than "intelligence."

- The fourth bullet addresses correlation of information and real-time monitoring of assets. While we agree that both are important, it is also important that this role be given to appropriate stakeholders and that roles and responsibilities be clarified. For example, it is important that owners and operators of critical infrastructure monitor their networks for malicious activity; however, this would be an unacceptable role for government to play. Furthermore, information sharing and correlation is important but must be done in a voluntary, collaborative manner, especially when private-sector data is involved.

- We strongly agree with the statement in the fifth bullet that India needs to "adopt counter measures on the basis of hierarchy of priority and understanding of the interdependencies, rather than attempting to defend against all intrusions and attacks." A risk-based approach, whose hallmark is to mitigate risk on the basis of the likelihood and impact of its realization, is a key element of any effective cyber security policy.

- We also strongly agree with the statement in the sixth bullet that the breadth of the issue of cyber security requires the consideration of the full spectrum of "people, process and technology." While technology is obviously a key component, too often cyber security policy focuses excessively on one factor at the expense of the others, producing less effective results.

- The final bullet in Section 1.4 states that 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." We agree with this policy consideration and recommend that the government examine not only how technology is designed and manufactured, but also how it is deployed and maintained. There are many existing international standards and best practices that address these issues and we encourage the GOI to actively leverage those resources. Furthermore, we note that public-private partnership frameworks help both government and industry better understand legal and technical capabilities, while creating a platform for better collaboration. We would like to engage with government representatives in a dialogue on how such efforts can be appropriately recognized. Our collective goal is to ensure that effective measures are in place and resources are better allocated towards that end, rather than in endless administrative revaluation of existing systems and processes.

D. Deloitte Touch Tohmatsu India Private Limited.

Section 1.4 can be moved as Glossary or Appendix

E. Internet and Mobile Association of India

Key Policy Considerations: While regulating cyber space, cyber space itself should be classified basis the nature of network access and information thereof. Accordingly security measures should be mandated for each classification.

F. Microsoft Corporation (India) Private Limited

The second bullet states that "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."

Comment: Indeed, cyber security does need to move beyond point solutions and technology alone. It must be dynamic, based on defence-in-depth, and, as stated later in this section, include people-, process-, and technology-based measures. In the second sentence, we recommend a greater focus on resiliency as it is not realistic to detect, stop and prevent *all* attacks. The idea of prevention, detection, response, and recovery would be more consistent with risk management and resiliency principles.
The third bullet point discusses the need to "adopt suitable counter measures and attribute the attacks for possible counter action."

Comment: Cyber intelligence is an integral component to help secure cyberspace, but the focus of attribution should not be limited to counter actions. Greater attribution will inform counter actions when necessary, but will also act as a deterrent and aid in law enforcement efforts to prosecute criminal behaviour.

The sixth bullet states: "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."

Comment: This statement is unclear as written. We suggest: "Security requires an effective combination of people, process and technology. It is important to focus on people and processes as much as technology because, without them, the technological measures alone would prove insufficient.
The eighth bullet states: "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"

Comment: The concept of "building-in" security is very important and perhaps should be moved up in the list. We also suggest that the statement also be updated to reflect both the need to "build-in" security as well as maintain security throughout the system lifecycle to address the rapidly changing technological and threat environments.

G. Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's

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.

- It is important to have necessary depth to detect, stop and prevent attacks through cyber security intelligence to anticipate attacks, adopt suitable counter measures and attribute the attacks for possible counter action. 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.

- It is important that owners and operators of critical infrastructure monitor their networks for malicious activity and keep the Government informed that they are taking all security measures

through their security policies and compliance. Furthermore, information sharing and correlation is important but must be done in a voluntary, collaborative manner, especially when private-sector data is involved.

- There are many existing international standards and best practices that address these issues and we request the Government to actively leverage those resources. We would like to engage with government representatives in a dialogue on how such efforts can be appropriately recognized. Our collective goal is to assure that effective measures are in place and resources are better allocated towards that end, rather than in frequent administrative revaluation of existing systems and processes.

H. FICCI

The third bullet in this section describes "cyber security intelligence" as an integral component of the security of cyberspace. While we agree with the intent of the statement—anticipate attacks, adopt suitable countermeasures and attribute the attacks for possible counter action—we suggest using the industry term of "situational awareness" rather than "intelligence."

Cyber intelligence is an integral component to help secure cyberspace, but the focus of attribution should not be limited to counter actions.

The fourth bullet addresses correlation of information and real-time monitoring of assets. While we agree that both are important, it is also important that this role be given to appropriate stakeholders and that roles and responsibilities be clarified. For example, it is important that owners and operators of critical infrastructure monitor their networks for malicious activity; however, this would be an unacceptable role for government to play. Furthermore, information sharing and correlation is important but must be done in a voluntary, collaborative manner, especially when private-sector data is involved.

We agree with the statement in the fifth bullet that India needs to "adopt counter measures on the basis of hierarchy of priority and understanding of the interdependencies, rather than attempting to defend against all intrusions and attacks." A risk-based approach, whose hallmark is to mitigate risk on the basis of the likelihood and impact of its realization, is a key element of any effective cyber security policy.

The sixth bullet states: "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, Therefore, "Security requires an effective combination of people, process and technologies."

The final bullet in Section 1.4 states that 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." We agree with this policy consideration and recommend that the government examine not only how technology is designed and manufactured, but also how it is deployed and maintained. There are many existing international standards and best practices that address these issues and we encourage the GOI to actively leverage those resources.

I. Safenet Inc

Section 1.4, first bullet: While this bullet refers to "impact on national security, public safety and economic well-being", is safe-guarding the individual rights (as empowered by Indian Constitution in the context of physical world) in the cyber space any part of the scope of this policy discussion? From one standpoint, I tend to think "public safety" is inclusive of "individual rights" but at the execution level I think any consideration towards "safeguarding individual rights" may completely be lost against the narrow definition of "public safety". Or, this being a National Security policy may not at all be meant to focus on individual rights.

Section 1.4, second bullet: a very well said statement as it is. Experiencing the interpretation at execution level, the only suggestion that comes to mind is to extend this statement to "It needs to be

dynamic in nature and have necessary depth to detect, stop and prevent attacks by putting in place multiple layers of technological as well as non-technological security measures with focus on data confidentiality, data integrity, non-repudiation, access control and traceability."

Clause 2.0 Cyber space – Nature of threat

Comments on Clause 2.0

A. Department of Telecommunications (Unit: Security)

The heading of the section 'Cyber space-Nature of Threat' could be changed to 'Dimensions of the Cyber Space'

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.

Comments on sub clause 2.1:

A. KR Information Security Solutions

May like to add the following:-

The easy availability coupled with the relatively low technological know-how required to use the malware implies that it is not just inimical entities that pose a threat but novices can also cause harm to our information infrastructure. This malicious activity can cause disruption/harm to our IT assets that are disproportionately high as compared to the efforts required.

B. **US India Business Council**

Comment: Section 2.1 correctly notes that cyber security threats are some of the most serious facing the global community. Importantly, the policy identifies the myriad victims of such attacks to include not just government and national infrastructure, but also individuals and businesses.

Indeed, the private sector must constantly adapt and evolve to meet enhanced cyber security threats. The ability of the private sector to protect its infrastructure against these new and evolving threats will depend, in large part, on a national framework/regulatory environment that provides flexibility and is adaptive as technologies and threats evolve. For example, companies need the flexibility to deploy strong encryption on their networks to deter increasingly sophisticated and disruptive cyber attacks. The government must therefore develop a support structure that encourages the deployment and use of strong encryption by the private sector.

At the same time, we also recognize the need for Indian Law Enforcement officials to detect and combat terrorists, criminals, and other nefarious groups who harness technology to do harm. It is important that future encryption regulations do not require companies to choose between either weak encryption or prior notice and decryption key escrow for stronger encryption. Requirements for companies, particularly Internet Service Providers (ISPs), to disclose encryption keys to government depositories could create a disincentive for companies to deploy robust encryption, which would ultimately increase India's overall Vulnerability to cyber attack. Notice and deposit requirements are not the norm in the regulatory environments of other jurisdictions.

As technology becomes a more integral part of daily life, governments, businesses, and individuals increasingly require a mechanism for protecting data from compromise by external parties. Thanks to the widespread commercial availability of encryption products, it is now possible to protect sensitive and important information and data. Clearly, however, the use of encryption poses important questions and challenges for law enforcement and national security. Many countries have encountered these challenges and have developed policies and processes that allow for the robust use of encryption to protect data and privacy while providing government information and data necessary for law enforcement and national security purposes.

Recommendations: As the Government finalizes its cyber security policy, it should consider the following elements related to encryption:

- While encryption of data can presently be achieved in numerous ways, innovators will find methods of applying it to the point that it will become ubiquitous. Government encryption regulations need to be flexible and adaptive to innovations in encryption technology.

- Privacy must be a core consideration as government executes its responsibility of providing safety and security to its citizens and the ability to protect data is a very important element of privacy.

- Industry can cooperate with law enforcement agencies in cyber security prevention and response provided there are clearly defined legal responsibilities and procedures.

- Appropriately established public private partnership mechanisms can also help facilitate such cooperation. Like in other geographies, industry is willing to comply with government requirements or requests for cooperation that are based on well-established, well-known due processes, and managed through a centralized judicial or quasi-judicial authority. Burdensome costs of numerous requests should ideally be shared or borne by the Government.

- The global nature of company operations and information flows will often mean that investigatory requests implicate information stored in multiple nations or impacting citizens of multiple nations. Compliance requests should factor this reality into developing globally recognized due process and disclosure procedures.

- Government should take the necessary steps to determine which entity possesses any decryption keys at issue. Legal requests should appropriately be made to the person or entity who has possession of the relevant keys for the encrypted communication or data and not to other tangential parties who may benefit from or touch the data but do not have the keys.

C. **Deloitte Touch Tohmatsu India Private Limited**.

Can be moved as Glossary or Appendix

D. **Microsoft Corporation (India) Private Limited**

"Threats emanate from a wide variety of sources, and manifest themselves in disruptive activities that target individuals, businesses, national infrastructures, and governments alike."
Comment: Consider that disruption may not be the only concern, especially for critical infrastructure. Incapacitation, exploitation or the loss of integrity are also concerns that should be addressed.
"Threat actors can operate with substantial impunity from virtually anywhere."

Comment: While there are many places where this may be true, it is too broad a generalization. Instead, we recommend discussing that the lack of identity, and sufficient and harmonized cybercrime legal frameworks in cyberspace impedes efforts to stop bad actors, and then highlighting this as a matter of international cooperation.

E. Software Freedom Law Centre

The policy document only gives a brief overview of the various forms of threats which are present in information networks. It does not enumerate the sources as well as the different categories of threats. Towards this, reference may be made to Para 2.1 of the Policy, which only provides a sparse overview of the, "threat landscape". In this regard, it is beneficial to look at the approaches followed by other countries and later adopt a policy which works both globally as well as locally.

The United Kingdom has published the "Cyber Security Strategy of the United Kingdom" in June, 2009 which devotes Chapter 2 to the identification of threats.[1] The policy first defines the source of these threats emanating from various persons such as, (a) criminals; (b) terrorists; (c) foreign states. It then proceeds to study the method of these attacks.

The United States has published the National Strategy to Secure Cyberspace[2] in February, 2003 which from page 5 till page 11 identifies various risks to Cyber Security. It also ranks threats under five levels.

The Australian Government has commissioned several studies[3] on the state of Cyber Security pursuant to which it has published a paper on Cyber Security Strategy.[4] These include threat identification and measures to tackle them.

Canada lists the various forms and sources of Cyber threats in its Cyber Security Strategy announced in 2010.[5]It also makes the use of statistics and relevant data to identify the threats and well as to suggest policy responses.

Germany's Cyber Security Strategy mentions threat assessment in the framework which has been drawn up by its Ministry of Interior.[6]

A presentation on the Cyber Security Policy of Japan, made by its National Information Security Centre similarly identifies ten risks through past cyber security incidents as well as the projected risks to information infrastructures [7]

1 Cabinet Office, Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space, (June, 2009) available at www.official-documents.gov.uk/document/cm76/7642/7642.pdf

2 Department of Homeland Affairs, National Strategy to Secure Cyberspace (Feb., 2003) available at http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

3 Child Health Promotion Research Centre, Review of Existing Australian and International Cyber-Safety Research (May, 2009) available at http://www.dbcde.gov.au/__data/assets/pdf_file/0004/119416/ECU_Review_of_existing_Australian_and_international_ cyber-safety_research.pdf

4 Australian Government, Cyber Security Strategy (2009) available at http://bit.ly/i9Ktsl.

5 Minister of Public Safety, *Canada's Cyber Security Strategy* (2010) available at http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf

6 Federal Ministry of Interior, *Cyber Security Strategy for Germany* (Feb., 2011) available at http://bit.ly/eeR1HJ

7 National Information Security Centre, *Cyber Security Policy of Japan* (Feb. 02, 2011) available at www.cipdubaindu.ae/download/Mitsutaka%20Otsu.pdf

Suggestions

- It is important for the policy to examine the level as well the extent of each threat. Only a comprehensive study which identifies the degree of risks and threats can lead to a beneficial cyber security policy absent a sense of paranoia.
- While examining these threats, they may be classified into distinct threat levels and categories.
- It is suggested that only the threats which threaten Government functions as well as critical network infrastructure may be included in this policy.

F. **Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's**

Section 2.1 correctly notes that cyber security threats are some of the most serious facing the global community. Importantly, the policy identifies the myriad victims of such attacks to include not just government and national infrastructure, but also individuals and businesses.

Indeed, the private sector must constantly adapt and evolve to meet enhanced cyber security threats. The ability of the private sector to protect its infrastructure against these new and evolving threats will depend, in large part, on a national framework/regulatory environment that provides flexibility and is adaptive as technologies and threats evolve.

The use of encryption is healthy for transactions, yet it poses important questions and challenges for law enforcement and national security. Many countries have encountered these challenges and have developed policies and processes that allow for the robust use of encryption to protect data and privacy while providing government information and data necessary for law enforcement and national security purposes. The Government can enhance skills, capability and capacities of their mechanisms through international cooperation at their level rather than individually by TSPs and ISPs.

G. **Department of Telecommunications (Unit: Security)**

Section 1.2 and 2.1 probably can be put together and need for action may be brought out more clearly.

H. **FICCI**

Threats emanate from a wide variety of sources, and manifest themselves in disruptive activities that target individuals, businesses, national infrastructures, and governments alike. Considering that disruption may not be the only concern, especially for critical infrastructure, Incapacitation, exploitation or the loss of integrity are also concerns that should be addressed. "Threat actors can operate with substantial impunity from virtually anywhere."

In the cyber space it is just one world, no countries, and no boundaries. There are two classes of people reside here, hackers and the rest. Hence threat landscape includes threats from all corners of the world.

The awareness among masses is possible and can be a cyber defence measure. This can be achieved by introducing relevant topics as a course in school/college curriculums A cyber watch Guard community can be built to educate kids/teens about necessary do's & don'ts of cyber communication.

Section correctly notes that cyber security threats are some of the most serious threats facing the global community. Importantly, the policy should identify the myriad victims of such attacks to include not just government and national infrastructure, but also individuals and businesses. Indeed, the private sector must constantly adapt and evolve to meet enhanced cyber security threats. The

ability of the private sector to protect its infrastructure against these new and evolving threats will depend, in large part, on a national framework/regulatory environment that provides flexibility and is adaptive as technologies and threats evolve.

At the same time, we must also recognize the need for Indian Law Enforcement officials to detect and combat terrorists, criminals, and other nefarious groups who harness technology to do harm. It is important that future encryption regulations do not require companies to choose between either weak encryption or prior notice and decryption key escrow for stronger encryption. Also notice and deposit requirements are not the norm in the regulatory environments of other jurisdictions.

Clearly, however, the use of encryption poses important questions and challenges for law enforcement and national security. Many countries have encountered these challenges and have developed policies and processes that allow for the robust use of encryption to protect data and privacy while providing government information and data necessary for law enforcement and national security purposes.

As the Government finalizes its cyber security policy, it should consider the following elements related to encryption: While encryption of data can presently be achieved in numerous ways, innovators will find methods of applying it to the point that it will become ubiquitous. Government encryption regulations need to be flexible and adaptive to innovations in encryption technology.

Privacy must be a core consideration as government executes its responsibility of providing safety and security to its citizens and the ability to protect data is a very important element of privacy.

Industry can cooperate with law enforcement agencies in cyber security prevention and response provided there are clearly defined legal responsibilities and procedures. Appropriately established public private partnership mechanisms can also help facilitate such cooperation. Like in other geographies, industry is willing to comply with government requirements or requests for cooperation that are based on well-established, well-known due processes, and managed through a centralized judicial or quasi-judicial authority. Burdensome costs of numerous requests should ideally be shared or borne by the Government.

The global nature of company operations and information flows will often mean that investigatory requests implicate information stored in multiple nations or impacting citizens of multiple nations. Compliance requests should factor this reality into developing globally recognized due process and disclosure procedures.

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.

Comments on subclause2.2:

A. US India Business Council

Comment: We strongly support the collaborative objectives of this section but are concerned that the section is too narrowly focused on supply chain. Furthermore, we warn of the possible danger of

conflating issues of supply chain provenance and malware. Preventing malware from being introduced into code is an issue to be dealt with in the context of the software development process. Preventing malware from being part of the supply chain goes to knowing the members of the supply chain and securing logistics channels. Both are important objectives, but they are accomplished in different ways and would suffer in a one-size-fits-all approach.

Recommendation: We suggest this section be broadened beyond issues of supply chain to recognize the need for international collaboration on a wide variety of cyber security issues.

B. **Deloitte Touch Tohmatsu India Private Limited**.

Can be moved as Glossary or Appendix

C. **Internet and Mobile Association of India**

So far as private sector is concerned, it role in co-operation should be limited to providing specific information for investigative reasons. Business Information / secrets should not be covered within the ambit of this policy.

D. **Microsoft Corporation (India) Private Limited**

This sections leads with the concern 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."

Comment: While the security of the ICT supply chain is an important concern, its placement in this section distracts from the equally important topic of international cooperation. We suggest that the discussion of ICT supply chain concerns should be moved to section 3.1, as a specific focus area in key action #3, revised as follows: "Process for national-level risk assessments, based on all-hazards threats (i.e., natural, accidents, and intentional acts) and considering key governmental concerns, such as the security of the ICT supply chain." The section should then have new text focusing on the need for greater international cooperation, identify some of the priority issues in this space for the Indian Government, and consider adding example forums for engagement.

E. **Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's**

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.

F. **United States Department of State**

The importance of international cooperation and aligning domestic policy with international best practices and norms. With increasing global connectivity, international norms, standards and cooperation play key roles in facilitating interoperability and enabling the effectiveness of the global Internet. Appropriate international cooperation and sharing of cyber security information are important means for addressing risks, threats, and incidents that cross national boundaries.

a) **Law Enforcement:** We encourage India's support for the Budapest Convention on Cybercrime as the only effective international model for domestic legislation and international cooperation on Cybercrime. Also, India should address its participation in the G8 24-7 network's role in this document International cooperation is essential for addressing Cybercrime that crosses national

boundaries. The policy document doesn't appear to cover "ordinary" or physical crime that is facilitated by computer networks or for which networks can furnish evidence. Whether the losses are financing corruption or terrorism, this kind of crime is an important concern.

b) **Leveraging the issue-specific work of other countries and established international forums:** The U.S. IT Sector Coordinating Council, for example, has developed a number of different strategies, including on supply-chain issues, which could be valuable. In addition, the US has developed documents like the National Information Protection Plan and the Strategy to Secure Control Systems which we would be willing to discuss with our Indian colleagues.

c) **International norms of behaviour:** Cooperation in the development of international norms guiding state behaviour in cyberspace- in times of peace and conflict – should be addressed as they will also contribute to increased cybersecurity. These norms include protection from crime, fundamental freedoms of expression and association and the right of self-defense.

d) **Research and development:** International cooperation in R&D efforts, along with cooperation with the private sector, can speed progress and increase the efficiency and effectiveness of solutions.

e) **Recognition of the threat of trusted insiders:** The international cooperation section has a focus on supply chain risk management and other global issues but does not appear to have recognition of the threat of trusted insiders which all countries face.

G. Infosys Technologies Limited

India as Signatory to International Conventions on cyber Security

The Policy says:

The Policy identifies international co-operation as an effective mechanism to control and address threats to cyber space.

Our view:

As identified in the policy, its objective of increased international cooperation for combating cyber offenses can be achieved by enhancing India's participation in international conventions on this subject. Cyber crimes as such do not respect any territorial boundary. As is true for any form of crime, enforcement is a key to control recurrence of cyber crime incidents which in turn can best be achieved by increased participation in international convention. The policy therefore may be used as an opportunity to form a strategy for making India a party to formal congregations on this subject (illustratively the Convention on Cybercrime) or to work towards inclusion of 'control of cybercrimes' as an agenda to the existing multi-national conventions.

H. **FICCI**

We support the collaborative objectives of this section but are concerned that the section is too narrowly focused on supply chain. Preventing malware from being introduced into code is an issue to be dealt with in the context of the software development process. Preventing malware from being part of the supply chain goes to knowing the members of the supply chain and securing logistics channels. Both are important objectives, but they are accomplished in different ways and would suffer in a one-size-fits-all approach. This section needs to be broadened beyond issues of supply chain to recognize the need for international collaboration on a wide variety of cyber security issues.

There should be greater emphasis and coordination between nations for enforceability of extra-territorial jurisdiction. Certain nations do not have extradition treaty due to which implementation of laws imposes a challenge. Nations should cooperate to establish an International Cyber Crime Tribunal.

I**. Information Technology Department Civil Secretariat, Srinagar/Jammu**

Scope, detail level and fields need to be defined, plus in an ever changing technological environment long term cooperation is sought, plus over dependency on international bodies without developing self-reliance and capacity building is a bad idea for the future.

2.3 Securing cyber space – Scope of action

Comments on subclause2.3

A. **Deloitte Touch Tohmatsu India Private Limited**.

Section 2.3 – Scope of Work

a. Should include the following –
   i. Introduce – People, Process, technology and other bullet points first up.
   ii. Give introductions to the major points which follow later on.
   iii. All general information can be mentioned in bullet points and rest can be moved to Appendices

---

2.3.1 Cyber security and cyber defence

Cyber security is the activity of protecting information and information systems (networks, computers, data bases, data centres 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 defence relates to a much more specialized activity linked to particular aspects and organizations. The distinguishing factors between cyber security and cyber defence 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 defence 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 defence environment requires deployment of technologies and capabilities for real-time protection and incident response. Generally, cyber defence is driven by intelligence on the threat to achieve the kind of defence 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 defence 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.

Comments on 2.3.1:

A. **Deloitte Touch Tohmatsu India Private Limited**.

Can be moved as Glossary or Appendix

B. **Microsoft Corporation (India) Private Limited**

Comment: This section introduces definitions of both cyber security and cyber defence. Related to the necessary international cooperation on this topic, it is important to harmonize the definitions of these terms. We suggest the Indian Government consider existing definitions for these terms from organizations such as the International Telecommunication Union (ITU) or the International Standards Organization (ISO) and work with industry to develop definitions to guide future policy.

C. Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's

The effectiveness of cyber defence 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. Government can play a proactive role and consult/advise the sector.

D. FICCI

Given the broad nature of cyber security and cyber defence, we recommend that Government shall consult closely with industry to develop more specific definitions and points of reference to help guide future policy, rules and regulations.

E. Safenet Inc

Section 2.3.1: refers to "Cyber Security is the activity of **protecting** information and information systems (networks, computers, data bases, data centres and applications)……"

a. Is it worthwhile defining the term "protecting" in specific and explicit terms. It is important that requisite information and information systems are "available", do not "lose any information and identities", and are "not susceptible to unauthorized/malign changes" despite faced with the hostile attacks. In that sense, protection has the key aspects of "Availability", "Data Confidentiality", "Data Integrity", "Non-Repudiation", "Access Control" and "Traceability" to hold.
b. including "identities" along with "networks, computers, data bases, data centers and applications" as the critical element to protect

---

2.3.2 Cyber intelligence and cyber defence

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. Skilful 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.

Comments on 2.3.2:

A. **Deloitte Touch Tohmatsu India Private Limited**.

Can be moved as Glossary or Appendix

B. **Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's**

The value of collecting intelligence information about threat sources and possible cyber attacks cannot be underestimated. We urge the Government to strengthen its intelligence gathering resources like CERT.in and keep the stakeholders also in confidence especially for the national level massive attacks, aimed at disabling the infrastructure rendering it unusable or inaccessible to users; or targeted attacks, aimed at collecting sensitive/strategic information.

Cyber defence relates to defensive actions against activities primarily originating from hostile actors with political or economic motivations, which could impact national security, public safety, or the economic well-being of the society. Given the broad nature of cyber security and cyber defence, we recommend that Government consult the industry to develop more specific definitions and points of reference to help guide future policy, rules and regulations.

C. **Department of Telecommunications (Unit: Security)**

The wordings in Para 2.3.2 does not seem to gel with the heading of the Para.

D. **Information Technology Department Civil Secretariat, Srinagar/Jammu**

A Unit / Team in constant research in Cyber Intelligence should be created on a permanent basis, for continuous intelligence inputs.

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 behaviour. 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 behaviour & 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.

Comments on sub clause 2.4:

A. Shri V. Vasant

To also indicate a time frame for implementation of the various initiatives/ policy measures laid out. At least a categorization into short-term, mid-term and long-term initiatives would be helpful in prioritizing the wide set of policy measures.

B. IIT Delhi

The document has delved on the generic cyber security background issues but fails to describe the prevailing situation in India with clarity. In absence of the clear articulation of current challenges the objective setting for short and long term objectives is not having required depth. In para 2.4 of document under 'Priorities for action' title the list of objectives are listed without any prioritization, quantified degree and time horizon.

C. KR Information Security Solutions

May like to include the requirement of development of resilient IT systems as attacks on these systems are more or less assumed to be omnipresent. We need networks and systems that continue to provide some level of efficiency even in the face of attacks.

D. US India Business Council

Comment: Section 2.4 states that "Indigenous development of suitable security techniques and technology through frontier technology research, solution oriented research, proof of concept, pilot development, etc. and deployment of security IT products/processes" is a priority. We applaud all governments' recognition of their critical roles in supporting research and development (R&D) of cyber security technologies. Cyber security is a fast paced race in which we must stay ahead of cyber criminals who adapt constantly. Cyber security policy should support and enable the development of the widest possible choice of cutting edge cyber security solutions. We have long encouraged the U.S. Government to increase its R&D in this area, to help identify R&D gaps and direct resources to emerging security technologies, and to support industry's R&D, and we similarly support India's recognition of this role for the GOI.

We support the continued growth of a globally competitive and innovative cyber security industry in India, and many of our members are contributing to that development. However, we are concerned that DIT may be attempting to give preferential treatment to the procurement of domestically produced or domestically owned technologies for India's cyber security. Such an approach could run afoul of India's trade commitments. It also could leave India less secure. India's businesses, consumers, and government entities should have access to the best available security technologies regardless of their country of origin. It would also diminish, rather than enhance India's attractiveness as an innovative and investment-friendly destination for foreign companies and reduce opportunities for collaborative efforts between Indian and foreign technology companies in the long-run.

Recommendation: We recommend that this section be amended to support the global development of security technologies through international collaboration and participation in international standards. The GOI needs to ensure that indigenous development of cyber techniques does not create a walled-garden effect for approaches to cyber security, which will ultimately lead to the country becoming less secure and potentially create interoperability problems with the rest of the world. Furthermore, while we support India's desire to enhance research and development in a number of the areas highlighted, this should not result in requirements favouring domestic sourcing, mandating transfers of technology or intellectual property, or otherwise skewing competition in the marketplace. We support reference in other parts of the plan to adhere to international standards and best practices and strongly encourage India to engage in international standards bodies working on different aspects of cyber security (e.g. ISO, CCRA).

E. **Deloitte Touch Tohmatsu India Private Limited**.

Putting in place 24 x 7 mechanism for cyber security emergency response & resolution and crisis management through effective predictive, preventive, protective, detective, corrective response and recovery actions -

Section 2.4

b. Can add information on forensics of events and/or incidents
c. Point number 7 can be merged with Point number 1
d. Point number 8 can be detailed with information on prevention and prosecution actions (or should refer to point number 2 on legal environment)

F. Internet and Mobile Association of India

Since this call for creating conducive legal environment in support of safe and secure cyber space, there is already an existing set of laws in the form of Information Technology Act and rules there under. If at all, the same law may be amended and new set of law need not be enacted for regulating the cyber space. This shall avoid confusion and multiplicity of laws.

G. **Microsoft Corporation (India) Private Limited**

Bullet six in this section states that "Indigenous development of suitable security techniques and technology through frontier technology research, solution oriented research, proof of concept, pilot development, etc. and deployment of security IT products/processes."

Comment: Microsoft supports, and contributes to, the development of indigenous capacity in India as a key component of economic development. Microsoft Research India has been focused on developing technology for emerging markets, multilingual systems, sensor networks and Geographical Information Systems since 2005. The statement from the draft, however, seems to imply that indigenous innovation will automatically produce more trustworthy or secure products and services. We anticipate the experts in DIT can appreciate that this is an erroneous and flawed presumption that could have the unintended consequence of reducing security. We support the Indian government's goal to deploy secure IT products/processes, and suggest that, that goal is best achieved by focusing on how products and services are produced using risk management, international standards, and transparent practices.

Bullet nine in this section states that "Proactive preventative and reactive mitigation actions to reach out and neutralize the sources of trouble and support for creation of global security ecosystem, including public-private partnership arrangements, information, sharing, bilateral and multilateral agreements with overseas CERTs, security agencies, and security vendors etc."

Comment: Microsoft supports the concepts in this bullet so strongly, we recommend splitting it into three bullets, to sufficiently highlight each. We suggest creating a bullet on proactive risk management actions and real-time situational awareness, to prevent, detect, and remediate issues; a second bullet on public-private partnerships and information sharing; and a third bullet on international cooperation, via bilateral and multi-lateral engagement.

H. Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's

Government may initiate

- Creation of necessary situational awareness regarding threats to ICT infrastructure for determination and implementation of suitable response
- Creation of a culture of cyber security for responsible user behaviour & 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.
    - Identify R&D gaps and direct resources to emerging security technologies, and to support industry's R&D.
    - Rather than inventing wheels the Government may liaison with experts elsewhere and those in India also.
    - India's businesses, consumers, and government entities should have access to the best available security technologies regardless of their country of origin.

I. Department of Telecommunications (Unit: Security)

There seems to be some overlapping between Para 2.4 and Para 3.1

J. Software Freedom Law Center

In this respect **Para 2.4** mentions that there is a need for the, "*protection of data while in processing handling, storage & transit and protection of sensitive personal information to create a necessary environment of trust*".

This paragraph which forms one of the few mentions on the importance of privacy of Internet users, does not mention the importance of regulating the circumstances of acquisition of the users data or sensitive personal information. The acquisition of the data and the sensitive personal information of the user needs to be dealt carefully by the government agencies or any other parties authorized to do so and strict penalties must be imposed on any misuse of such data. Governments all over the world have been concerned about collection of sensitive information such as health records, location based records and services, mining of personal information for commercial purposes. Such activities without proper safeguards could open a plethora of problems.

Similarly, **Para 2.4** which states that there should be a focus on, "*creation of a culture of cyber security for responsible user behaviour & actions*" should be suitably amended. Here it is important that, "*responsible user behaviour & actions*" should not lead to intermediaries blocking access and services to persons utilizing pseudonyms to avail a certain level of online anonymity.

Also, whenever any blocking of information is carried out it should be as per the provisions of the Information Technology Act, 2000. Moreover, it is suggested in cases, when such blocking is ordered through a government authority, such an order should be made publicly available on the Ministry of Information Technology's website.

Hence, it important for the Cyber Security Alert as issued by CERT-in to be detailed as well mention the grounds of opinion why the alert has been issued. It should also mention to whom it applies. In a sense it should clearly mark out the applicable class of Government organizations/service providers, to whom the cyber security alert is most relevant.

K. **FICCI**

Bullet six in this section states that "Indigenous development of suitable security techniques and technology through frontier technology research, solution oriented research, proof of concept, pilot development, etc. and deployment of security IT products/processes."

We believe that this section be further amended to support the global development of security technologies through international collaboration and participation in international standards. The GOI also needs to ensure that indigenous development of cyber techniques does not create a restricted

boundary effect for approaches to cyber security. It would also diminish, rather than enhance India's attractiveness as an innovative and investment-friendly destination for foreign companies and reduce opportunities for collaborative efforts between Indian and foreign technology companies in the long-run.

India shall plan to adhere to international standards and best practices. India's businesses, consumers, and government entities should have access to the best available security technologies regardless of their country of origin

L. Safenet Inc

Section 2.4 – Priorities for action: I would say that this is the "core" of this policy document and as such it shall define the specifics along with the inter-dependencies, responsibilities and overall time bound roadmap. Following thoughts come to my mind:

a. The first and foremost action item shall be of that of creating an "organization structure" within the Government of India for the purpose of Cyber Security. It does seem that CERT-In is coordinating with a plethora of other departments within GOI but it is not clear as to who owns the ultimate responsibility – is it CERT-In or is CERT-In just a consultative body with no ownership. Irrespective, I think we first need to have an effective organization structure in place to address it.
b. Once the organization structure is in place then this organization shall lay out the overall roadmap for the finalization and subsequent implementation of this policy. It is not clear as of now as to how will we evaluate ourselves on the progress made or lack there-of as go forward in time
c. Said differently, there has to be a legislation conferring it the powers to effectively execute it.

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.

Comments on sub clause 2.5:

A. KR Information Security Solutions

This section states that the first priority for the government is to identify the most dangerous classes of cyber security threats. It is felt that rather than identifying the threats (as these are evolving in nature),

the government must concentrate on identifying the critical systems and data that needs protection and then to mandate the level of protection required for these assets

B. **Microsoft Corporation (India) Private Limited**

Comment: Effective public private partnerships require strong participation by both government and industry. This section, as written, is overly weighted towards government capabilities while overlooking the role of industry. We suggest revising this section to position government and industry as partners working together to manage risk. Specifically, the text specifies, "Government should identify the most dangerous classes of cyber security threats, the most critical IT infrastructure vulnerabilities, and the most difficult cyber security problems" This type of risk management activity is best carried out as a joint activity between government and industry, as each has unique expertise and understanding of these factors. Further, while appropriately highlighting risk management activities, we recommend using a risk assessment approach that lead with an assessment of consequences of concern, followed by vulnerabilities, and then threats instead of the reverse. This approach has been found to be more effective for information infrastructure because the consequences of concern are least likely to change over time, while the threats are so dynamic and varied they are often difficult to catalog and even the most creative minds will not think of all the possibilities. Finally the sentence "Public-private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery operations." can be simplified as "Public-private engagement will take a variety of forms and will address policy, operations, and technology", and possibly supplemented with examples of each.

C. **Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's**

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. Public-private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery operations.

D. United States Department of State

Importance of the public/private partnerships: We appreciate the recognition that all stakeholders have a role to play in developing a cultural of cyber security. The Government of India has made great strides regarding inclusion of the private sector. However, in the development and implementation of domestic cyber policies, close coordination with private businesses encourages risk reduction within their own organizations and also provides vital insight into the development of appropriate government policies. This is also true in the development of CERTs, the development and prioritization of threats, and other important issues. A key piece of the draft's priorities for international cooperation would require public-private partnerships for successful execution. We recommend that this be stated outright.

Clause 3.0 Enabling processes

Comments on Clause3.0

A. **Deloitte Touch Tohmatsu India Private Limited**.

We are talking about enabling Process, Technology and People. We can think of introducing this aspect in section 2.3 Scope of Work

B. **Government of Andhra Pradesh, IT&C Department, Infrastructure Wing**

1. Policy may propose Information Security Standards for accessing / processing information through
    a) Integrated Wireless and Wired networks
    b) Integrated Sensor (such as RFID), Wireless and Wired networks

2. Policy may recommend Information Security guidelines and standards for eGovernance projects executed under PPP framework or otherwise

3. Policy may recommend establishing an office of CISO at each state level which can co-ordinate with CERT-In and with Sector level CERTs for uniform implementation & monitoring of National Cyber Security Policy

4. The office of the state level CISO may be staffed / supported by suitably qualified and trained/certified (CISSP, CISA, CCNA) officers from NIC, CDAC, State Government / Public Sector Organizations

5. Policy may propose a unified Information Security Assessment Framework enough to cater to all sectors of Indian Society – from Government Organizations, through private ISPs to Individual citizens (Self-assessment in the case of Individual Citizens)

6. Policy may establish the mandatory and recommendatory periodicity of Cyber Security Audits for Government sector

7. Policy may recommend the establishment & maintenance of knowledge Network related to Cyber Security by CERT-In, collaboration with Academic Institutions, State CISO offices, and Sectoral CERTs for sharing of 'Best practices' , Cyber Attack resolutions & Trend analysis of past cyber attacks.

8. Periodic privacy Impact assessment (PIA) of all organizations acquiring Citizens' personal information to be mandated and the results of the PIAs to be published

9. Policy may use OECD's 8 principles for privacy protection
    1. Collection Limitation principle
    2. Data quality principle
    3. Purpose Specification principle
    4. Use Limitation principle
    5. Security Safeguards principle
    6. Openness principle
    7. Individual participation principle
    8. Accountability principle

    for establishing PIA standards

10. PIA to be in conformance with relevant sections of the proposed EDS Bill 2011, IT Act 2000 & 2008 Amendments

11. Policy may recommend periodic Information Safety Awareness campaigns to be undertaken by office of State CISO through multiple channels (e.g. TV, Mobile, Internet, Print Media etc)

12. Policy may establish Data quality and Data protection standards for Government Information in conformance with the proposed Electronic Delivery of Services Bill 2011 and IT Act of 2000 and 2008 Amendments

13. Policy may ensure that guidelines / recommendation proposed under National cyber Security Policy are consistent with Right To Information Act 2005

14. Policy may recommend guidelines for establishing Disaster Recovery and Business Continuity mechanisms for critical sectors of the Government

15. Policy may recommend Information Archival & Retrieval guidelines for Critical Sectors of the government

C. **FICCI**

Governments need to make fighting cyber crime a priority by efficiently and effectively enforcing cyber crime laws, including allocating adequate resources to enforce cyber crime laws:

- Law enforcement personnel need to be trained about sophisticated cyber crime.
- Law enforcement also needs adequate equipment to conduct investigations.

Law enforcement action must also take place across borders. Law enforcement agencies need to build networks of relationships with their counterparts in other countries and regions.

While creating legal frameworks about data protection and privacy, consideration should be given whether requirements would be appropriate to protect personally identifiable information against unauthorized access and disclosure.

Governments should maintain a policy of technology neutrality when they develop cyber security policies and laws. Security information sharing and cooperation can be done in strong partnership with private software organizations.

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 Centres, 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*.

Comments on sub clause 3.1:

A. AKS Information Technology Services Private Ltd.

For
Development of comprehensive repair and maintenance policy so as to minimize false alarm and increase cyber resource availability to all users efficiently.
Should be
Development of comprehensive repair and maintenance policy so as to minimize recovery time and increase cyber resource availability to all users efficiently.

B. KR Information Security Solutions

Point 5 of this section provides for the identification of a national level security organisation to act as the nodal agency for all matters pertaining to Information Security in the country. Sec 70 (b) of IT Act (Amdt) 2008 already caters to this provision. Additionally there are other organisations (such as NTRO) that are also mandated to carry out national level information security functions. There appears to be some confusion as to the overlapping roles of these organisations. This Security Policy document must therefore, clarify this confusion rather than enhancing it.

May also like to add a provision for mandatory periodic testing and evaluation of the security controls of the IT infrastructure of critical infrastructure even in the private sector.

C. STQC

Also include risk assessment as a formal process (Reference ISO 27005)

D: US India Business Council

Comment (1): Section 3.1 correctly notes that much of the responsibility for network security will fall upon non-governmental actors. In order to ensure that "facility owners" and other non-governmental actors have the means to execute their "responsibility to limit or manage risks from these threats to the extent possible," government policies must give the private sector the flexibility to deploy the most advanced and state-of-the art technology to protect critical ICT infrastructure. Given the global nature of threats, the private sector has a strong incentive to integrate solutions based on global best practices. Any future government rules should take into account the need and desire of non-governmental partners to draw upon global technology and procedures in defending their networks.

Comment (2): Section 3.1 also states that the "use of secure products/services, protocols & communications, trusted networks and digital control systems" are key actions to reduce security threats and related vulnerabilities. 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."

It is unclear how "secure information flows" would be measured, what the expectations would be, and how this would be enforced. India could enhance the framework for collaboration if soliciting cooperation from the private sector for matters of law enforcement if based on transparency and proper adherence to the rule of law. Clear and understandable regulatory frameworks developed with stakeholder input will ensure that all requests are conducted in a manner consistent with India's legal framework for lawful intercept, privacy, and respect for individual rights. As noted above, industry stands ready to comply with government requirements or requests for cooperation that are based on well-established, well-known due processes, and managed through a centralized judicial or quasi-judicial authority. Burdensome costs of numerous requests should ideally be shared or borne by the Government.

Section 3.1 also proposes "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." We agree that it is important to have an appropriate level of assurance that critical information infrastructure facilities and assets are able to withstand cyber attacks. What level of assurance is appropriate, what cyber attacks are facilities and assets required to withstand, to what degree they are required to withstand such attacks, and how and by whom the ability is verified are questions that raise a host of legal and operational issues of considerable importance.

To address these issues, we strongly recommend that a collaborative approach between the government and the relevant companies be used.

E. **Deloitte Touch Tohmatsu India Private Limited**.

Point 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.
Question: Shouldn't it include periodic vulnerability assessment of critical information infrastructure

Section 3.1

Can add bullet point after 4; information on actions to be taken after detection/assessment of damages – what should be enforced or what should be instigated

F. **Microsoft Corporation (India) Private Limited**

Comment: Managing risk is critical activity to help improve the security of the information infrastructure, and this section appropriately highlights that need. Again, we recommend a few revisions that would facilitate a risk management approach appropriately tailored and effective for the unique characteristics of the information infrastructure. First, the interconnected nature of the multitude of systems and networks that make up the information infrastructure makes taking a "facility" "asset" based approach impractical. Instead, we recommend the Indian Government focus on the ICT functions and systems it relies upon. Second, we suggest that the text call to "reduce risks" rather than "reduce vulnerabilities" and for "risk assessments" rather than "threat and vulnerability assessments" as risk mitigations may exist in all three risk factors, threat, vulnerability, and consequence. We offered a specific revision provided in our comments on section 2.2 to moving the supply chain concerns to section 3.1 key action #3, revised as follows: "Process for national-level risk {revised from threat and vulnerability} assessments, based on all-hazards (i.e., natural, accidents, and intentional acts) and considering key governmental concerns, such as the security of the ICT supply chain."

"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."

Comment: Verification of emergency preparedness is best managed by using conformance with international standards and generally accepted auditing procedures, such as ISO 14000 and 27000 series.

G. **Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's**

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:

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

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

- Identification and classification of critical information infrastructure facilities and assets.

- Roadmaps for organization-wise security policy implementation in line with international security best practices standards and other related guidelines.

- Process for national level security threat & vulnerability assessments to understand the potential consequences.

- 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.

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

- Periodic 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.

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

- Given the global nature of threats, the private sector has a strong incentive to integrate solutions based on global best practices.

- Any future government rules should take into account the need and desire of non-governmental partners to draw upon global technology and procedures in defending their networks.

- As noted above, Industry stands ready to comply with government requirements or requests for cooperation that are based on well-established, well-known due processes, and managed through a centralized judicial or quasi-judicial authority. Burdensome costs of numerous requests should ideally be shared or borne by the Government.

H. **Department of Telecommunications (Unit: Security)**

There seems to be some overlapping between Para 2.4 and Para 3.1

I. **FICCI**

Section correctly notes that much of the responsibility for network security will fall upon non-governmental actors. In order to ensure that "facility owners" and other non-governmental actors have the means to execute their "responsibility to limit or manage risks from these threats to the extent possible," government policies must give the private sector the flexibility to deploy the most advanced and state-of-the art technology to protect critical ICT infrastructure. Given the global nature of threats, the private sector has a strong incentive to integrate solutions based on global best practices. Any future government rules should take into account the need and desire of non-governmental partners to draw upon global technology and procedures in defending their networks.

Section 3.1 also states that the "use of secure products/services, protocols & communications, trusted networks and digital control systems" are key actions to reduce security threats and related vulnerabilities. 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."

It is unclear how "secure information flows" would be measured, what the expectations would be, and how this would be enforced. India could enhance the framework for collaboration if soliciting cooperation from the private sector for matters of law enforcement if based on transparency and proper adherence to the rule of law. Clear and understandable regulatory frameworks developed with stakeholder input will ensure that all requests are conducted in a manner consistent with India's legal framework for lawful intercept, privacy, and respect for individual rights.

Section 3.1 also proposes "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." We agree that it is important to have an appropriate level of assurance that critical information infrastructure facilities and assets are able to withstand cyber attacks. What level of assurance is appropriate, what cyber attacks are facilities and assets required to withstand, to what degree they are required to withstand such attacks, and how and by whom the ability is verified are questions that raise a host of legal and operational issues of considerable importance. To address these issues, we strongly recommend that a collaborative approach between the government and the relevant companies be used.

J. **Information Technology Department Civil Secretariat, Srinagar/Jammu**

Regarding "key action" (4) Standards should be defined for product and services, standardization of IT Infrastructure in key installation should be considered.

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.

Comments on sub clause 3.2 (a):

A. AKS Information Technology Services Private Ltd

Para 3.2 (ii)

The following points may also be included under National Cyber Alert System:-

- Creation of honeynets for capturing attack signatures and understanding trends of malware development for taking timely preventive measures.
- Internet monitoring at National Gateways.
- Monitoring of Cyber Cafés.
- Development of database of attackers source IPs for black-listing and blocking at Firewall.

B. **Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's**

National cyber alert system

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. 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.

- It is important to have clear policies and procedures for designation of critical infrastructure and, in particular, of how non-governmental sectors are chosen as critical infrastructure sectors and effectiveness be factored.
- Government agencies should lead by example in terms of securing their own networks, we are concerned Departments' information security policies and guidelines that are developed or applied in an uncoordinated or inconsistent manner could lead to conflicting or unattainable requirements for vendors that sell to the Indian Government.
- To meet its security goals for government information infrastructure, we suggest that India consider moving toward a common set of information security functional requirements for its Departments.
- Having all Departments use the same baseline requirements will give them a greater selection of vendors and technologies that meet their needs.

C. Government of West Bengal

Regarding Para 3.2 a) National Cyber Alert System, mentions the need to have a quick information exchange mechanism on early warning and response information between Centre and States. In the Policy document, more elaboration may be placed on the roadmap to put up such a system in place.

---

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.

Comments on sub clause 3.2 (b):

A. Infosys Technologies Limited

The policy says:

In order to effectively deal with targeted cyber attacks in sensitive and strategic sectors, the policy envisages setting up of sectoral CERTs who would be responsible for incidence resolution.

Our View:

The policy adopts a hub and spoke model in the form of having national nodal agency in CERT-In and sectoral CERTs for the different critical sectors. It however currently prescribes the sectors CERTs to play a role in incidence resolution only. We believe that requiring such agencies to adopt a proactive role in identifying, controlling and preventing occurrence of incidents of cyber security lapses will allow the policy to be more fully aligned with the objectives underlying the policy. Illustratively, these agencies could study emerging threats in cyber security space, collaborate with similar existing agencies in other countries as also with players in private sector to formulate a stronger framework to combat threats to cyber security. The policy may therefore consider providing these additional prescriptions for the sectoral CERTs.

B. Government of West Bengal

Regarding Para 3.2 b) Sectoral CERTs, it is suggested to have Nodal Officers in critical departments at State level to coordinate with sector CERTs at Central level for preventing and reactive actions.

---

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*.

Comments on subclause3.2 (c):

3.3 Security best practices -compliance and assurance

Comments on sub clause 3.3

A. KR Information Security Solutions

In Section 3.3, Security best practices - compliance and assurance under the sub-section 'E-Governance' it says that "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." These remarks should not appear in a Policy document which aims to lay down the exact requirements that must be met by organisations.

B. Internet and Mobile Association of India

This mandates best security practices for critical sectors. The definition of critical sectors should be limited to such sectors which may affect national security or may lead to loss of life. Pure business ventures should not be covered under this definition / policy.

C. Software Freedom Law Center

Provisions regarding security practices and procedures to be implemented by organizations that handle sensitive personal data or information are laid out in Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. The rules require such organizations to implement "security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business" (sic). International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements" is a standard on Information security prescribed by the rules. Intermediaries, including telecom service providers, network service providers, INTERNET service providers, web-hosting service providers, search engines, on-line payment sites, on-line auction sites, online market places and cyber cafes, have to comply with such procedures as per the provisions of Information Technology (Intermediaries guidelines) Rules, 2011 .

This is a statutory requirement that has to be complied by such organizations. The policy, without any statutory basis, cannot require organizations to adopt any procedure beyond those mandated by statutory provisions.

Also if under the Policy, any such restrictions are imposed on organizations (intermediaries, large corporates, small and medium users) as well as regulations of operations should be based on statutory provisions. Such actions cannot be undertaken through clauses in a policy document. CERT has only limited powers under Sec. 70B of the IT Act. The policy mentions cyber security intelligence and conducting of surprise vulnerability checks (**Page 9, Para 3.3**) but the statute does not seem to provide the legal sanction for such actions.

(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

Comments on subclause3.3,(i) (a):

A. Information Technology Department Secretariat, Chennai

The information of electronic files pertaining to Government / Critical sectors may be classified as Top Secret, Secret, Confidential, Restricted and Public.

B. STQC

Add:

a) Develop business continuity management framework (including emergency response, disaster recovery and business continuity.
b) Configuration audits of critical systems and network devices.
c) Desktop audits

C Deloitte Touch Tohmatsu India Private Limited

- Subsection (a) – Can elaborate on the bullet points and add more as required. We can add information on virtualization (Cloud Security Assessment) etc.
- Hotspot (wi-fi) Security
- Security in relation to the Internet Service Provider (Broadband and DSL) – there were a few cases in the past where terrorists misused the wi-fi router of citizens, so this is probably more of ISP's responsibility.
- Information Security Incident Management may be mentioned.
- War dialing, intrusion, interception, etc. also may be mentioned.
- One of the biggest threats that need to be considered is putting controls on Cyber Café – nothing in relation to that is mentioned.
- Privacy is mentioned but not clear.

- The policy can have Cyber Security attack alert levels (for e.g. 1 to 4 or critical, High, medium, low) to let the nation know what criticality of danger the country is currently facing (if under attack)
- The policy may talk about setting up a nationwide dedicated helpline or email or portal for reporting cyber security attacks and giving information.
- The policy may setup a para-legal framework to expedite cyber terrorism cases.
- The policy may setup a mock/replica/test facility with similar resources as CERT-in but open to public who wish to participate in investigating and helping the govt. on cyber security issues.
- The policy may have strict rules for recruitment (for e.g. No prior history of convictions or criminal record or use of illegal drugs, mandatory polygraph tests, mandatory certifications and test scores, etc.,)

D. Microsoft Corporation (India) Private Limited

"Government and critical sectors organizations are required to do the following on priority."

Comment: We strongly support the many of the priority actions in the section, and encourage using such a "baseline" of security controls based on international standards, at each level across the Indian Government. The application these requirements in critical infrastructures, however, needs to be further explored before inclusion as it is not yet clear from the document what comprises critical infrastructure nor what the full implications of that designation are. For example, communications is generally considered a critical infrastructure sector, but the communications infrastructure itself is comprised of widely varying access devices (e.g., cell phones, tablets), equipment (e.g., routers and switches), systems, networks, and providers that interact and change dynamically, have varying criticality, and require different levels and types of protection.

"Report to CERT-In cyber security incidents…"

Comment: It is critically important to carefully define reporting requirements for cyber-security incidents, as not all events are of similar significance and meaning (imagine the loss of laptop versus that of the transport capabilities to a specific region of the country). Having too much data that doesn't have meaning and without the necessary computing or human capability to analyze it is equally concerning as having insufficient data. Operational information sharing is a challenging issue, and is most often successful when information is shared to focus on a specific outcome that is mutually beneficial to both parties, such as government sharing information on national security threats with the private sector to help secure the supply chain. If developed, information sharing requests should ensure privacy and protection of confidential information of customers and the private sector (e.g., trade secrets, intellectual property).

E. Safenet Inc

Section 3.3 (i) (a).4 refers to tests that seem to focus at the specific elements (breaching the parameter and breaching the application) rather than the entirety (which is the protection of data and identities). Anyways, I think it is too general and instead shall seek to work towards standards that are applicable for specific departments/scenarios.

F. Information Technology Department Civil Secretariat, Srinagar/Jammu

Continuous training for team handling critical cyber infrastructure must be made mandatory.

(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.

Comments on subclause3.3, (i) (b):

A. Information Technology Department Secretariat, Chennai

Data pertaining to Government Departments/ Undertakings should be migrated to State Data Certres (SDC) and Communications should be done only using State Wide Area Networks (SWAN)

(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.

Comments on subclause3.3, (i) (c):

Comments on subclause3.3, (i), a, b & c

A. **US India Business Council**

Comment: The discussion draft envisages a quasi-regulatory framework to govern the cyber security of critical information infrastructure. It is important that the infrastructure to which this framework applies is not excessively broad. We otherwise run the risk of overstretching the resources of the government agencies tasked with its oversight. We would also impose a potentially cumbersome set of obligations on companies that own or operate infrastructure that is not genuinely critical. We recommend that the criteria used for the designation of critical information infrastructure be clear and appropriately narrow. Additionally, it is important to have clear policies and procedures for designation of critical infrastructure and, in particular, for how non-governmental sectors are chosen as critical infrastructure sectors. For example, is the designation for the entire sector or only some aspects and what are the implications of the inclusion? This is important because of the implications of section 3.3(i) (a) on the ability of companies to use existing, possibly global and currently deployed security practices and methods to test and evaluate those requirements as appropriate. Changes in these current practices may implicate legal or contractual requirements already in place. What form of consultation with owners and operators of such infrastructure and flexible application is being considered? What due process is available to companies wishing to challenge their designation as critical infrastructure? Similar questions would be raised related to what would be qualifications of independent auditors and against what standard(s) they would be auditing. What would the role of internal audit be and how would issues of cost-benefit and effectiveness be factored?

This section also states that 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." While we agree that government agencies should lead by example in terms of securing their own networks, we are concerned Departments' information security policies and guidelines that are developed or applied in an

uncoordinated or inconsistent manner could lead to conflicting or unattainable requirements for vendors that sell to the Indian Government.

Finally, this section requires critical infrastructure companies to "report to CERT-IN cyber security incidents, as and when they occur and the status of cyber security, periodically." We caution against imposing overbroad obligations to share operational security information. Such obligations may run against the need for organizations to comply with incompatible legal requirements (e.g. privacy), and to protect their confidential information and communications and that of their customers, trade secrets, intellectual property, etc. We recommend that the GoI work with industry to establish clear guidelines about such sharing of information.

Recommendation: To meet its security goals for government information infrastructure, we suggest that India consider moving toward a common set of information security functional requirements for its Departments, with disparate requirements for "national security" networks- e.g. military/intelligence networks, and "non-national security" networks. These would include some fundamental outcome-based requirements such as data protection and increased awareness of network activity.

If such an approach is adopted, India should make every effort to ensure that all Departments articulate security functional requirements consistently. Departments may have unique characteristics and security needs that require them to take security measures above and beyond the common requirements. However, having all Departments use the same baseline requirements will give them a greater selection of vendors and technologies that meet their needs.

We further suggest that the scope of crucial infrastructure be clearly defined in the cyber security policy.

B. <u>FICCI</u>

The discussion draft envisages a quasi-regulatory framework to govern the cyber security of critical information infrastructure. It is important that the infrastructure to which this framework applies is not excessively broad. Additionally, it is important to have clear policies and procedures for designation of critical infrastructure. We recommend that the GoI work with industry to establish clear guidelines about such sharing of information.

It is not yet clear from the document what comprises neither critical infrastructure nor what the full implications of that designation are. It is critically important to carefully define reporting requirements for cyber-security incidents. Information sharing requests should ensure privacy and protection of confidential information of customers and the private sector (e.g., trade secrets, intellectual property).

To meet its security goals for government information infrastructure, we suggest that India consider moving toward a common set of information security functional requirements for its Departments, with disparate requirements for "national security" networks- e.g. military/intelligence networks, and "non-national security" networks. These would include some fundamental outcome-based requirements such as data protection and increased awareness of network activity. If such an approach is adopted, India should make every effort to ensure that all Departments articulate security functional requirements consistently. Departments may have unique characteristics and security needs that require them to take security measures above and beyond the common requirements. However, having all Departments use the same baseline requirements will give them a greater selection of vendors and technologies that meet their needs. The scope of crucial infrastructure be clearly defined in the cyber security policy.

(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.

Comments on subclause3.3,(ii)

A. Microsoft Corporation (India) Private Limited

"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."

Comment: Microsoft believes in the principle of "trust but verify", but is uncertain about the compliance regime established in this section. The concepts and interplay between the "Information Security Assurance Framework", the "National Security Policy Compliance Requirements", and "National Conformity Assessment infrastructure", are unclear and need to be more thoroughly explored. Additional information on how the requirements would be developed, what are the concerns to address, and how and to whom they will be apply needs to be documented. We believe that international standards and existing certification regimes, such as the International Organization for Standardization 27000 series, should be the primary mechanisms to verify compliance with security requirements.

***(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.*

Comments on subclause3.3, (ii) (a):

***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.*

Comments on subclause3.3, (ii), (b):

A. **STQC**

Endorsing actions are meant to assure conformance of all the enabling actions, therefore, it can be a separate section covering endorsement of 3.3 I to IV, 3.4, 3.5, 4.0, 5.0 etc.

Endorsement actions (Assessment of certification) (3.3 ii, b)
Add:
Compliance to IT Acts/ Rules

Endorsement actions (IT Security Product Evaluation and Certification reference)
Add:
Reference to Common Criteria standard (ISO/IEC 15408) with minimum assurance level EAL2 for IT products to be used for low risk environment.

Comments on subclause3.3, (ii), a & b

A. US India Business Council

Comment: We support the implementation of effective information security practices and mechanisms. However, there is insufficient information to determine how these National Security Compliance requirements will be developed, what they might be comprised of, and how they will be applied.

Recommendation: We strongly urge the GOI to provide clarity on the following issues:

- The role of industry in the development of any information security practices and mechanisms;
- Plans for leveraging/incorporating/recognizing existing practices and certifications like the Common Criteria;
- What international standards will CERT-In use in its assessments and certifications and to what extent will those requirements apply to privately owned systems and networks; and
- The scope of the endorsing actions and how they will be applied – for example, use of terms like "compliance with international standards," as opposed to "adoption and implementation of national approaches?"

B. **Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's**

Information security Assurance Framework-Enabling and Endorsing actions

- We support the implementation of effective information security practices and mechanisms. However, there is insufficient information to determine how these National Information Security Compliance requirements will be developed, what they might be comprised of, and how they will be applied.

- We suggest the Government to provide clarity on the following issues:

  - What will be the role of industry in their development;
  - How will they leverage/incorporate/recognize existing practices and certifications like the Common Criteria;
  - What international standards will CERT-IN use in its assessments and certifications and to what extent will those requirements apply to privately owned systems and networks; and
  - What are the endorsing actions and how they will be applied – for example, use of terms like "compliance with international standards", as opposed to "adoption and implementation of national approaches"?

C. **FICCI**

We support the implementation of effective information security practices and mechanisms. However, there is insufficient information to determine how these National Security Compliance requirements will be developed, what they might be comprised of, and how they will be applied.
We strongly urge the GOI to provide clarity on the following issues:

- The role of industry in the development of any information security practices and mechanisms;
- Plans for leveraging/incorporating/recognizing existing practices and certifications like the Common Criteria;
- What international standards will CERT-In use in its assessments and certifications and to what extent will those requirements apply to privately owned systems and networks;
- The scope of the endorsing actions and how they will be applied – for example, use of terms like "compliance with international standards," as opposed to "adoption and implementation of national approaches?"

"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."

(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.

Comments on subclause3.3,(ii) (c):

A. **US India Business Council**

Comment: We strongly agree with the paper's statement that business entities must develop and implement adequate levels of trust and confidence in the realm of privacy and data protection in order to stay globally competitive. To that end, a balanced privacy bill will help support India's economic growth and development and will encourage foreign companies to continue to rely upon India as a global destination for business process outsourcing, data processing, and research and development. We believe, however, that any future legislation that imposes an unduly restrictive privacy regime will severely undermine the thriving IT and Business Process Outsourcing industry that has contributed greatly to India's economic development and growth.

Recommendation: Future privacy legislation should include several important foundations and protections for the collection, storage, and use of personal information. Specifically, any legislation should (1) recognize that the free flow of information is critical to the continued growth and vitality of the global economy, specifically for India and (2) be flexible enough to allow India to develop approaches to privacy consistent with other countries and multilateral organizations and bodies.

B. **Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's**

Data Security and Privacy Protection for 'Trust and Confidence 'Comment:

- We agree with the paper's statement that business entities must develop and implement adequate levels of trust & confidence in the realm of privacy and data protection in order to stay globally competitive.

- To that end, a balanced privacy policy will help support India's economic growth and development and will encourage foreign companies to continue to rely upon India as a global destination for business process outsourcing, data handling, and research and development.

C. **FICCI**

We agree with the paper's statement that business entities must develop and implement adequate levels of trust and confidence in the realm of privacy and data protection in order to stay globally competitive. To that end, a balanced privacy bill will help support India's economic growth and development and will encourage foreign companies to continue to rely upon India as a global destination for business process outsourcing, data processing, and research and development. We believe, however, that any future legislation that imposes an unduly restrictive privacy regime will severely undermine the thriving IT and Business Process Outsourcing industry that has contributed greatly to India's economic development and growth.

Future privacy legislation should include several important foundations and protections for the collection, storage, and use of personal information. Specifically, any legislation should (1) recognize that the free flow of information is critical to the continued growth and vitality of the global economy, specifically for India and (2) be flexible enough to allow India to develop approaches to privacy consistent with other countries and multilateral organizations and bodies.

D. **Internet and Mobile Association of India**

A separate privacy and data security framework may not be required under this policy since the same is mandated under various rules framed under Information Technology Act.

E. **Information Technology Department Civil Secretariat, Srinagar/Jammu**

All sections of IT Users whether Government or Business Entities should be responsible for privacy protection and Data Security, unlike only Business Entities in the draft.

(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.

Comments on subclause3.3, (ii) (d):

A. Information Technology Department Secretariat, Chennai

Para 3.3, (ii), (d) : Quality and protection of electronic records: Formal Processes need to be in place for disposal of old IT equipment and usage of storage devices.

B. **Software Freedom Law Center**

This para broadly calls for extensive data retention. Here several issues will need to be examined, including, (a) whether the network service provider may legally create user logs for each user; (b) what types of data and under what circumstances will the network service provider have to store data; (c) can such data be stored even if the user specifically requests its deletion; (d) if yes, what will be the period of retention of such data; (e) if the data is retained then is the retention same for all forms of data; (f) how long may back-ups of data be retained despite the specific request of the user to delete it. These issues have a heavy interplay with privacy regulation and hence, data retention as a concern will require independent scrutiny.

Suggestions

- Since the policy is concerned with national Cyber Security it should identify critical infrastructure and then take actions to protect it. This will usually cover a lot of Government

infrastructure and where private players control such infrastructures, the Central Government should only prescribe minimum guidelines which does not interfere immensely with their ability to operate. The Government can take steps to help such private players in their Cyber Security needs, and hence their needs for cyber security technology also the Government can take long-term actions to increase the quality and availability of Cyber Security technologies available in the marketplace.

- Bringing small and medium users like individuals and small and medium enterprises and businesses in the policy ambit may impose excessive regulation and the need to use costly software on them without benefit to Cyber Security. They should be excluded from the policy ambit.

- Independent and detailed study is called for issues such as encryption and data retention involving all effected stakeholders. A policy of forbearance should be adopted with respect to these highly topical subjects in the Cyber Security Policy.

- **Para 3.3(ii)(d)** which states, that electronic records should be protected from "falsification". This may even imply that each electronic record may be matched against an individual user and may lead to legal controls against pseudonymous and anonymous online activity. This may not only endanger privacy but also will have a chilling effect on online free speech and expression.

Comments on subclause3.3, (ii) (c) & (d):

A. STQC

Data security and privacy protection for trust and confidence and Quality and protection of electronic record : These enabling actions are also to be covered under the endorsement actions.

(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.

Comments on subclause3.3, (iii):

A. **US India Business Council**

Comment: We agree with the statement that e-governance initiatives should be based on best information security practices. However, encouraging only Public Key Infrastructure (PKI) could skew departments to adopt a single technology, while ignoring other solutions that may meet their security needs.

Recommendation: Revise this section to encourage wider adoption of technologies and best practices, and in the spirit of technology neutrality it should discourage departments from falling into the trap of technology mandates that will likely become outdated or obsolete.

B. **Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's**

E-governance

- We agree with the statement that e-governance initiatives should be based on best information security practices.
- Government may like to re-write this section to encourage wider adoption of technologies and best practices, and in the spirit of technology neutrality it should discourage departments from falling into a "favorite technology" trap.

C. FICCI

We agree with the statement that e-governance initiatives should be based on best information security practices. However, encouraging only Public Key Infrastructure (PKI) could skew departments to adopt a single technology, while ignoring other solutions that may meet their security needs.

It is important to revise this section to encourage wider adoption of technologies and best practices, and in the spirit of technology neutrality.

D. Information Technology Department Civil Secretariat, Srinagar/Jammu

E-Governance projects when conceived and approved should address Security and Privacy issues while developing the projects, this component should be made mandatory for all upcoming projects.

(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.

Comments on subclause 3.3, (IV):

A. **STQC**

The section on secure software development and application - IV – Can also be covered under endorsement actions

B. **US India Business Council**

Comment: This section includes a provision that software development processes must be "supervised and monitored." We are concerned that this could provide an unprecedented level of oversight into private sector operations and that it does not recognize the efforts of many vendors and associations to adequately develop secure software based on customer requirements and market imperatives.

This section also appears to conflate the concept of open source and open standards. Generally, open standards refers to how standards are developed – in an open, consensus driven and voluntary manner, with reasonable and non-discriminatory treatment of intellectual property (IP) – as well as to their availability in sufficient detail to enable a complete understanding of their scope and purpose to enable competing implementations by multiple vendors. Open Source means that there is no IP owner of the technology – and that parties contribute to creating and improving it without expectation of any IP rights. TIA and USIBC recognize the validity of both concepts. We believe that government and private-sector decisions about products and technologies should be made in a technology neutral

manner that weighs the relative merits of any technology, without policy preference for one over the other. As it is impossible to predict how any specific solution will fare in the marketplace, policies should encourage competition between standards through voluntary, market-driven processes.

Recommendations:

- India should recognize and promote industry-led efforts to develop and implement secure software development.
- This section should be refined to include a discussion of open standards separate from issues of open source. We further recommend that the discussion be broadened to a discussion of "global standards" developed in an open, consensus driven and voluntary manner. The use of "global standards" allows for the flexibility of recognizing a variety of standards development organizations that operate globally.

C. **Deloitte Touch Tohmatsu India Private Limited**.

Can include Conduction of secure code reviews to be part of the development phase
The public and private key transactions can be introduced to perform electronic transactions.
There should be two way authentication mechanisms in electronic transactions.
All the transaction should be encrypted.
Captcha should be introduced to perform the each transaction.

D. **Microsoft Corporation (India) Private Limited**

"Software development process, whether in-house or outsourced, needs to be supervised and monitored using a system development lifecycle methodology."

Comment: Microsoft strongly supports the focus on secure development lifecycle processes; the Microsoft Security Development Lifecycle is required for all our products and services, and we share the process, practices, and tools with the ecosystem globally to promote usage. A policy requiring supervision or monitoring of development processes will neither scale across the ecosystem and is unlikely to produce meaningful results. While international standards do not yet exist for this requirement, we believe that market demand is driving increased industry adoption, and that the market can be further incentivized with governmental procurements policy favoring organizations that self-attest to using secure development practices and can demonstrate artifacts (e.g., corporate policy, documentation, tooling) of that.

Open Standards
"To minimize the risk of dependency on proprietary IT products, open standards need to be encouraged."

The idea of open standards appears to be confused with open source, although both are valid concepts. Microsoft supports open standards, which typically refers to standards developed using an open, consensus-based process and which are accessible and usable by multiple vendors. Microsoft also supports the use of both proprietary and open source software and services, and encourages a technology-neutral policy where the merits of any technology can be equally considered without preference for one or the other.

E. **Tata Teleservices Limited And Tata Teleservices (Maharashtra) Limited's**

Secure software development and application

- India should recognize and promote industry-led efforts to develop and implement secure software development.
- This section should be refined to include a discussion of open standards separate from issues of open source.

F. Software Freedom Law Centre:

Open Standards compliance should be a necessary component of a comprehensive national Cyber security policy and not merely to "be encouraged"

The draft policy suggests that compliance with relevant open standards be "encouraged" as part of the effort to make government computer networks, solutions, workstations and devices more secure. In fact, DIT has already called for mandatory open standards http://egovstandards.gov.in/notification/Notification_Policy_on_Open_Standards_-_12Nov10.pdf/view compliance to be used in e-governance applications to ensure sharing of information and seamless interoperability of data across applications. Although the Cyber Security policy mentions the need to encourage open standards, in the light of the policy on open standards, it is imperative that open standards are made mandatory. In the area of information security, proprietary standards with its closed nature could lead to security risks and vendor lock-in and have to be avoided.

More important, however, is the necessary role open standards play in securing Government Information Technology (IT). As the draft policy notes, the most important procurement goal is that IT security be "designed in" rather than "bolted on" what Governments buy and use. Open Standards compliance means compliance with standards that have been produced in a standards process that maximizes public participation and review of implementation, including open source implementation. Open standards openly developed are far more likely to take security into account throughout the design and definition process than programs or solutions represented by a single, proprietary implementation. For this reason, although open standards compliance is nowhere near sufficient to establish "security designed in," it is in practice a necessary component of such an outcome.

G. **United States Department of State**

Open Standards: The recognition of the importance of open standards is important for the continued development of the IT sector in India. However, in this document there is ambiguity regarding whether the term "open standards" refers to the series of technical specification enabling software to be used across diverse platforms or open source software, which has no intellectual property owner and source code available to be modified at any party. We recommend further clarification on this. As companies continue to drive innovation in the development of proprietary software, countries should also highlight the vibrancy of the open source software movement.

H.. **Infosys Technologies Limited**

The Policy says:

While discussing the measures for enabling the technology for fortifying cyber security, the Policy recommends use of open standards as it would minimize risks of dependency on proprietary IT products. In this recommendation, the Policy does not enumerate in greater detail about what constitutes 'open standards'.

Our view:
As currently described, it is not clear whether the term 'open standards' refer to system applications developed in a 'free for all' environment or to 'standardized specifications' (e.g. – encryption standards, communication protocols) for critical systems that are made known to the public at large. While the latter is a welcome step and will lead to a uniform, transparent and reinforced environment for critical system, the former may pose challenges for the government/critical sector in balancing the benefits of having open standards vis-a-vis having a security procedure that ensures control over design, specifications, ownership and secrecy.

Therefore to achieve better clarity and direction, the scope of the term 'open standards' may be explained in the Policy.

I. **FICCI**

This section includes a provision that software development processes must be "supervised and monitored." We are concerned that this could provide an unprecedented level of oversight into private sector operations and that it does not recognize the efforts of many vendors and associations to adequately develop secure software based on customer requirements and market imperatives.

This section also appears to conflate the concept of open source and open standards. We believe that government and private-sector decisions about products and technologies should be made in a technology neutral manner that weighs the relative merits of any technology, without policy preference for one over the other. As it is impossible to predict how any specific solution will fare in the marketplace, policies should encourage competition between standards through voluntary, market-driven processes.

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*.

Comments on subclause3.4*:*

A. **Tata Teleservices Limited And Tata Teleservices (Maharashtra) Limited's**

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.
- As noted above, the ability of the private sector to protect its infrastructure against new and evolving threats and cooperate with the Government on law enforcement and intelligence matters will depend, in large part, on a national framework/regulatory environment that provides flexibility and is adaptive as technologies and threats evolve. We recognize the need for Indian Law Enforcement officials to detect and combat terrorists, criminals, and other nefarious groups who harness technology to do harm. But it is important that industry and government collaborate to

create effective processes for the sharing of information based through well-established judicial processes.

B. **Information Technology Department Civil Secretariat, Srinagar/Jammu**

The plan does not seem to articulate the incident response process, and measures that must be followed when an attack is detected. Proper mechanisms be developed to address these issues.

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*

Comments on 3.5*:*

A. FICCI

There is a need for Indian Law Enforcement officials to detect and combat terrorists, criminals, and other nefarious groups who harness technology to do harm. For this it is important that industry and government collaborate to create effective processes for the sharing of information based through well-established judicial processes.

- Establish a National Centre for Computer Crime Complaints. Its key functions should be to receive on-line complaints, analyze them to identify the trends in internet crimes and refer the potential criminal schemes to the Centre/State law-enforcement agencies. This Centre should follow the single-window concept for identifying the criminal schemes for appropriate enforcement. It can also provide the forensic investigative and analytical support to all law-enforcement and regulatory agencies on a nationwide basis.
- Support and develop cyber security forensic capabilities. Create legal awareness on collections of electronic evidence. The adoption of the latest techniques of cyber forensics is essential in order to ensure conclusive investigation and prosecution of a cyber crime, Collection of electronic evidence is a challenge as information is intangible in nature and the electronic information has to be systematically captured in order to be produced and proved in a court of law.
- Consider constituting Cyber Crime Courts for expeditious trials.

Comments on subclause3.5.1*:*

A. **US India Business Council**

Recommendation: Section 3.5 notes that the IT Act Amendments of 2008 and their implementation regulations "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."

As noted above, the ability of the private sector to protect its infrastructure against new and evolving threats and cooperate with the Government on law enforcement and intelligence matters will depend, in large part, on a national framework/regulatory environment that provides flexibility and is adaptive as technologies and threats evolve. We recognize the need for Indian Law Enforcement officials to detect and combat terrorists, criminals, and other nefarious groups who harness technology to do harm. But it is important that industry and government collaborate to create effective processes for the sharing of information based through a well-established judicial processes.

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.

Comments on subclause3.5.2*:*

A. **Information Technology Department Civil Secretariat, Srinagar/Jammu**

Review of legal laws as per international trend is recommended.

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*

Comments on sub clause 3.6:

A. **Tata Teleservices Limited And Tata Teleservices (Maharashtra) Limited's**

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

---

Clause 4.0 Enabling technologies – Deployment and R&D

Comments on clause 4.0

A. **Deloitte Touch Tohmatsu India Private Limited**.

We are talking about enabling Process, Technology and People. We can think of introducing this aspect in section 2.3 Scope of Work

B. **Government of Andhra Pradesh, IT&C Department, Infrastructure Wing**

Enabling Technologies:

1. Policy may recommend prevention and Detection Technologies based on Defense-in-Depth strategy, for critical sectors in the Government

2. Policy may recommend transition to IPv6 protocol for better Cyber Security features

C. **FICCI**

Research and Development departments of many IT companies which focus on Security can be breeding ground for R&D work on the thrust areas as mentioned in the policy document.

Governments should support cyber security innovation through education and research and development (R&D). Governments should support the development and generalization of cyber security curricula in university-level IT education.

Government support of cyber security R&D helps meet the future technological needs of each country's infrastructure, as well as help each country develops its IT industry.

Governments should support cyber security R&D through public funding of basic and long term research. They should limit their involvement in applied R&D to circumstances where the technological solution that is sought is not commercially available, and its absence creates a measurable security gap – thus focusing government resources on long-term need.

Governments should also consider creating incentives that encourage the private sector to conduct cyber security R&D. IT Industry can participate in security specifications formulations, R&D and development of indigenous products.

Second major reason for undertaking indigenous R&D is to build confidence that an imported security product itself does not turn out to be a veiled security threat. The above statement from the draft seems

to imply that indigenous innovation will automatically produce more trustworthy or secure products and services. We anticipate the experts in DIT can appreciate that this is not an entirely valid presumption that could have the unintended consequence of reducing security threat vis-à-vis an imported product. We support the Indian government's goal to deploy secure IT products/processes, and suggest that, that goal is best achieved by focusing on how products and services are produced using risk management, international standards, and transparent practices.

Programs of research at universities, market-based financing of initiatives, and creating favorable conditions for companies to invest in local plants or to develop local capacity are all legitimate and acceptable government activities that do not rely on preferential treatment, limits on competition, or other processes that thwart the balance of markets. Forced technology transfer has been shown to be counterproductive in increasing a country's ability to expand commerce and increase its technical capabilities. In such cases, IPR holders will often forego market opportunities to retain their technology lead. This means that the government imposing such a provision will diminish its industry's access to the latest technologies and thus negatively impact the security of its own digital infrastructure.

While we recognize the desire of the Indian government to help create an enabling environment for the domestic development of technology, we urge the government to avoid developing "indigenous innovation" policies that seek to block foreign competition.

India needs to ensure that indigenous development of cyber techniques does not create a walled garden approach to cyber security, which will ultimately lead to India being less secure, while potentially creating interoperability problems with the rest of the world.

We recommend that any future cyber security policy not seek to achieve security through indigenous innovation or manufacturing. The geography of design or manufacture of products has not proven to be a fair or adequate measure of the security assurance of the product as even local or "indigenous" products can suffer from coding errors or vulnerabilities.

D. **Tata Teleservices Limited And Tata Teleservices (Maharashtra) Limited's**

we suggest that as referred in other parts of the plan to adhere to international standards and best practices and strongly encourage India to engage in international standards bodies working on different aspects of cyber security work.

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, defence-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.

Comments on sub clause 4.1:

A. **US India Business Council**

Comment: According to international standards (e.g. ITU-T X.800 and X.805), threats focus on five key areas: (1) destruction, (2) corruption, (3) disclosure, (4) removal or theft, and (5) interruption.

Our member companies can help provide cutting-edge and sophisticated technology to the Indian government for cyber security and law enforcement purposes. For example, an existing platform for the sharing of such information and for government procurement already exists through the USIBC/AMCHAM Homeland Security Working Group, which has been closely engaged with the Ministry of Home Affairs.

Recommendation: Leverage and expand existing platforms for collaboration (working groups etc.) to address the specific cyber security needs of the Indian government.

B. **Microsoft Corporation (India) Private Limited**

The first bullet in the list notes "implementing technologies throughout a layered, defense in depth strategy."

Comment: We are supportive of using layered defense in depth strategies and suggest only that the phrase "risk based" be added as well.

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 inhouse R&D, this sector may find it attractive to undertake collaborative R&D with leading research organizations.

Comments on sub clause 4.2.1:

A. **US India Business Council**

Comment: While we recognize the desire of the Indian government to help create an enabling environment for the domestic development of technology, we urge the government to avoid developing "indigenous innovation" policies that seek to block foreign competition. India needs to ensure that indigenous development of cyber techniques does not create a walled garden approach to cyber security, which will ultimately lead to India being less secure, while potentially creating interoperability problems with the rest of the world. We support references in other parts of the plan to

adhere to international standards and best practices and strongly encourage India to engage in international standards bodies working on different aspects of cyber security work (e.g. ISO/IEC, ITU, IETF, and CCRA).

The desire to build local industry capacity in critical infrastructure areas is not at issue, only the means. Programs of research at universities, market-based financing of initiatives, and creating favourable conditions for companies to invest in local plants or to develop local capacity are all legitimate and acceptable government activities that do not rely on skewed procurement requirements, limits on competition, or other processes that thwart the balance of markets. Forced technology transfer has been shown to be counterproductive in increasing a country's ability to expand commerce and increase its technical capabilities. In such cases, IPR holders will often forego market opportunities to retain their technology lead. This means that the government imposing such a provision will diminish its industry's access to the latest technologies and thus negatively impact the security of its own digital infrastructure.

Recommendation: We recommend that any future cyber security policy not seek to achieve security through indigenous innovation or manufacturing. The geography of design or manufacture of products has not proven to be a fair or adequate measure of the security assurance of the product as even local or "indigenous" products can suffer from coding errors or vulnerabilities.

B. **Microsoft Corporation (India) Private Limited**

"Second major reason for undertaking [indigenous] R&D is to build confidence that an imported security product itself does not turn out to be a veiled security threat.

Comment: Microsoft supports, and contributes to, the development of indigenous capacity in India as a key component of economic development. Microsoft Research India has been focused on developing technology for emerging markets, multilingual systems, sensor networks and Geographical Information Systems since 2005. This statement, however, seems to imply that indigenous innovation will produce more trustworthy or secure products and services. We anticipate the experts in DIT can appreciate that this is an erroneous and flawed presumption that could have the unintended consequence of reducing security. We support the Indian government's goal to deploy secure IT products/processes, and suggest that that goal is best achieved by focusing on how products and services are produced using risk management, international standards, and transparent practices.

C. Software Freedom Law Center:

The policy lays emphasis on indigenous Reseach & Development (R&D) as imported IT products could turn out to be a veiled security threat. The problem lies in the fact that equipments and software with proprietary source code do not offer an opportunity for auditing and verifying the source code for any malicious code or security loop holes. The answer to such concerns is to lay emphasis on FOSS based products as it provides an opportunity to verify and audit the underlying source code for any security threat. The Government has already invested in R&D activities in the area of FOSS through institutions like C-DAC, NIC and NRCFOSS. Such research can be effectively utilized in the R&D efforts visualized in the area of Cyber Security. Hence the policy could make a special mention of FOSS in the area of R&D as well as software deployment. As the policy rightly points out, collaboration among nations, the private sector and civil society is important in the matter of Cyber Security and FOSS projects with its inherent collaborative nature provides the ideal platform for this.

D. **United States Department of State**

Indigenous R&D: While we recognize the desire of the Indian Government to help create an enabling environment for the domestic development of technology, we urge the government to avoid developing "indigenous innovation" policies that seek to block foreign competition. India needs to ensure that indigenous development of cyber techniques does not create a walled garden approach to cyber security, which will ultimately lead to India being less secure, while potentially creating

interoperability problems with the rest of the world. Clarifying that technologies and equipment will be primarily reviewed for effectiveness and technical suitability versus country of origin would resolve potential trade conflicts and improve India's general security status.

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.

Comments on sub clause 4.2.2:

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.*

Comments on sub clause 4.2.3:

A. AKS Information Technology Services Private Ltd.

Thrust areas of R&D may also include:-

- Indigenous development of Indian Operating System (IOS).
- Indigenous development of web browser.
- Indigenous development of a Search Engine, like Google.
- Indigenous development of Indian Office software like MS Office.
- Indigenous development of critical applications.
- Steganography & Steganalysis.
- Indigenous Antimalware software.
- Development of database of IPs and ASN for profiling of targets.

Clause 5.0 Enabling people

Comments on clause 5.0

A. **Deloitte Touch Tohmatsu India Private Limited**.

We are talking about enabling Process, Technology and People. We can think of introducing this aspect in section 2.3 Scope of Work

B. **Government of Andhra Pradesh, IT&C Department, Infrastructure Wing**

Policy nay recommend training programs for different levels of Government staff in the Critical sectors of the Government, appropriate to their role in ensuring Cyber Security.

C. **FICCI**

Security skills training and certification can be achieved by leveraging the experience base of private software organizations.

Governments should tap industry resources for such efforts because industry – and the IT industry in particular – have developed a great deal of educational cyber security material, have marketing expertise and have established channels to communicate with the public.

The IT industry will have to pay a significant role to enable the Government to achieve its objectives through this framework. Significant among them are as under:

a. Creation of a strong talent pool in Information security.
b. Promote widely recognized professional information security certifications.
c. Setup security training infrastructure across the country for an effective outreach.

Governments need to educate the public – home users, children and small businesses in particular – about — cyber hygiene, safe and ethical computing. This includes education about software piracy, because many risks to the public come from the use of pirated software.

5.1 Security education and awareness

Comments on sub clause 5.1:

A. **Tata Teleservices Limited And Tata Teleservices (Maharashtra) Limited's**

Leverage and expand existing platforms for collaboration (working groups etc.) to address the specific

---

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.*

Comments on sub clause 5.1.1:

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*

Comments on sub clause 5.1.2:

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.

Comments on sub clause 5.1.3:

A. Software Freedom Law Center

Para 5.1.3 prescribes various measures which can be undertaken for the safe use of IT for children and small & home users.

It states that, "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"

If these concerns *qua* the vulnerability of children has to be addressed then it needs to be addressed through specific and separate legislations. It is also pertinent to mention that these measures, though may be commendable, fall outside the purview of cyber security. Such measures require independent study and a consultative process of their own.

B. Information Technology Department Civil Secretariat, Srinagar/Jammu

Specific campaigns for children & Home users should be a priority, campaign in Schools and Colleges is recommended.

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*

Comments on sub clause 5.2:

A. Government of West Bengal

Regarding Para 5.2 Security skills training and certifications, it is suggested that Sectoral CERTs create a pool of master trainers with expertise in various cyber security roles mentioned in the policy. These master trainers may subsequently train personnel in critical sectors in State Goverments

---

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 organizatins to have an effective outreach.

Comments on sub clause 5.3:

Clause 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.

Comments on clause 6.0

A. US India Business Council

Comment: This section states that large corporations must show "compliance to international security best practices and demonstration." There are a multitude of international security best practices available to corporations and other entities. These entities must have the discretion to choose which practices meet their particular needs.

Recommendation: We urge the GOI not to mandate compliance with any particular standard or best practices but to allow flexibility for industry to implement the practices that are best suited to their business and their customers' needs. We also are concerned that the draft is not clear as to how "compliance" will be enforced. In terms of language, we believe that it may be more appropriate to require that organizations be able to demonstrate the appropriate implementation and deployment of policies, practices and technologies, based on international standards, to address the risks associated with the type of business they engage in, specific customer security requirements, and information they handle.

B. **FICCI**

Large Corporates may contribute by sharing their best practices and capability with Govt. This section states that large corporations must show "compliance to international security best practices and demonstration." There is a large no. of international security best practices available to corporations

and other entities. These entities must have the discretion to choose which practices meet their particular needs.

We believe that the GOI not to mandate compliance with any particular standard or best practices but to allow flexibility for industry to implement the practices that are best suited to their business and their customers' needs.

Compliance to international security best practices may lead to significant expenditure on security technologies and processes. Governments should facilitate this information sharing by supporting the creation of public, private and joint capabilities. This includes both human and technical resources, as well as appropriate legal protections against anti-trust claims, disclosure requirements, etc. Governments should promote the development and adoption of industry best practices on information sharing.

Governments should build capacity to facilitate the sharing of cyber security information among companies and between the government and private sector (e.g. actionable threat information, response plans, etc.) Information sharing can enhance the protection of critical information infrastructure, most of which is owned and operated by the private sector:

Governments should address any policy or legal barriers that may inhibit information sharing. However, information sharing must be voluntary. Any obligation to share data would run against the need for organizations to comply with incompatible legal requirements (such as privacy laws, wherever they are applicable), and protect their confidential information, that of their customers, trade secrets, their intellectual property, etc.

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.*

Comments on sub clause 6.1:

A. **Microsoft Corporation (India) Private Limited**

This section states that large corporations must show "compliance to international security best practices and demonstration."

Comment: The compliance requirements need to be more well-defined, as there are innumerable best practices for security, and managing dynamic and evolving cyber risk requires flexibility and agility. We believe that international standards and existing certification regimes, such as the International Organization for Standardization 27000 series, should be the primary mechanisms to verify compliance with security requirements.

B. Software Freedom Law Centre:

In this respect, reference may be had to**, Para 6.1** which states that actions by network service providers should, "conform to legal obligations and cooperate with law enforcement activities including prompt actions on alert/advisories issued by CERT-in". **Para 3.1 (bullet 4)** states that, "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".

This is contrary to the current state of law as laid out in Sec. 69 of the IT Act and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 formed thereunder. Sec. 69 as well as provisions of the rules do not contemplate for any private agreements to be entered with intermediaries or network service providers. They only allow actions through orders which are issued in specific circumstances.

The policy exceeds this objective in prescribing actions for network service providers, large corporates, small/medium users and home users and by mentioning monitoring and surprise check mechanisms. A policy does not involve law making and hence new restrictions/ requirements apart from those laid out in statutes cannot be incorporated in it.

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' behaviour in the interest of safe computing both within and outside.*

Comments on sub clause 6.2:

A. **Software Freedom Law Center**

Para 6.2 which states that actions by large Corporates should "promote acceptable users behavior in the interest of safe computing both within and outside" should be redrafted with deletion of the term, "acceptable behavior".

B. **Tata Teleservices Limited and Tata Teleservices (Maharashtra) Limited's**

This section states that large corporations must show "compliance to international security best practices and demonstration." There are a multitude of international security best practices available to corporations and other entities. These entities must have the discretion to choose which practices meet their particular needs depending upon the business they handle.

Comments on subclauses 6.1 and 6.2:

A. Software Freedom Law Center

Para 6.1 and **Para 6.2** contain various actions which should be carried out by Network Service

Providers (specifically Internet Service Providers) and by large Corporates respectively. One of these action points state that, "*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.*" These acts, specifically "*net traffic monitoring*" may involve the monitoring and collection of user logs which may even contain their browsing history. This will result in substantial privacy violations and is against the constitutional mandates of the right to privacy. This is because such general pro-active measures cannot be taken when a person's privacy is involved. Invasion of a person's privacy is allowed under law, only on a case to case basis by issuing a specific order. Here reference may be made to the Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data of Information) Rules, 2009. The rules clearly contemplate under Rule 3(2), that, "*no directions for monitoring and collection of traffic data or information under sub-section (3) of section 69B of the Act shall be issued, except by an order made by the competent authority.*" Hence, these rules which are specifically formed to govern "net traffic monitoring", do not contemplate any, "pro-active measures", but prescribe passivity for Network Service Providers. This inherent passivity is only interfered on the basis of a specific order which is issued on the grounds and the procedures which have been prescribed under the Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data of Information) Rules, 2009. Such orders should reflect the constitutional concern for privacy as emphasized by the Hon'ble Supreme Court in the telephone tapping case.[9] Also, on May 11, 2011 the Hon'be Supreme Court made observations with respect to the right of privacy and responsibility of the network service provider when a request is made by any Government agency to tap telephonic conversations. This was done in the case of Member of the Parliament, Sh. Amar Singh wherein while criticizing Reliance Infocomm for tapping Sh. Singh's phone on the basis of 'forged' documents, the Hon'ble Court observed , "… the service provider has to act as a responsible agency and cannot act on any communication." The Hon'ble Court also asked the government to frame guidelines for the interception of telephone conversations to prevent illegal tapping by service providers. In view of the aforementioned observations by the Hon'ble Court, it is clear that the law of the land requires strict adherence to the fundamental rights enshrined in the Constitution which include the Right to Privacy with respect to both the wired as well as the wireless network.

Maintenance of user logs and the retention of data beyond the purpose for fulfilling the technical function as requested by the user poses a great privacy risk. This becomes incredibly relevant in light of the recent Ratan Tata privacy litigation in the Supreme Court, where the issue is not the legality of the telephone tapping but the unauthorized dissemination of the tapped conversations. Here the periods and the conditions under which data may be retained is important to be chalked out. In this respect the recommendation for independent study of data retention standards and clearer guidelines is restated.

9 Peoples Union for Civil Liberties v. Union of India (1997) 1 S.C.C. 301.

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.*

Comments on sub clause 6.3:

A. **Software Freedom Law Center**

a. **Para 6.3** recommends several measures which include, "*use legal software and update at regular intervals*". In a country like India, where a very large number of instances of unlicensed software usage have been reported due to high price of proprietary software, it is important for the government to encourage us of Free and Open Source Software which is verifiable, auditable. Proprietary software, which is mass produced and only provides minimum level of security dependent upon the market demand without much regard to a comprehensive security structure which encompasses concerns of the users as well does not give either the users or the Government any control over its structure and makes it difficult to built in security frameworks.

b. Issues such as content monitoring, data retention, encryption, child safety etc. are ancillary issues which though may be linked to Cyber Security require independent scrutiny and examination. If the policy goes ahead with maintaining references to them, it is advisable that it may be clarified that separate studies and policy documents may be taken out with respect to them.

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 throughout 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 National Cyber Security Policy, draft v1.0, 26 Mar 2011 20 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.

Comments on Annexure I:

A. IIT Delhi

The annexure-I describes stakeholder agencies without showing any linkages between them. There could be an organization structure at national level showing their dependency relationship and salient areas of responsibilities. The present description gives an impression that no apex body is really

responsible for national cyber security and various stakeholders are islands without essential linkages amongst them.

B. **Safenet Inc**

Coming to organization structure or stake-holders, shouldn't Ministry of HRD be a key stake-holder in devising and executing the programs at elementary school, graduate and post graduate level to facilitate the requisite skill sets and awareness that is critical to success of this Cyber Security Policy

How do we expect to defend against the attacks if we do not have the courses that help build professionals in the areas of Cryptology, Crypto-analysis, Ethical Hacking etc?

C. Data Security Council of India (DSCI)

Though the draft policy identifies some of the stakeholders agencies (Annexure I), there is a need to identify all the stakeholders including those from the private sector and establish linkages between them (roles & responsibilities, co-ordination, co-operation, collaboration, information sharing, etc.).

Software Freedom Law Center

Executive Summary

The policy in its current state is a crucial first step towards creation of a suitable cyber security ecosystem in the country. However, the policy must take into account the following considerations in order to devise a comprehensive approach and strategy for protection of Cyber space in India.

1. Detailed study and description of the threat landscape should be carried out in line with the approach followed by other countries;

2. The focus of the policy should be on critical infrastructure;

3. Software running critical services and infrastructure should be audit-able and verifiable by the Government and capable of "designing in" requisite security measures; Cyber Security requires verifiable software engineering practices and thus the policy should mandate them; Crucial nature of the mobile network governance should be considered and made a part of a comprehensive policy;

4. Open Standards compliance should be a necessary component of a comprehensive national Cyber security policy;

5. The Policy should determine the role the government should play in the defense of critical infrastructures, while safeguarding privacy and civil liberties;

6. The Policy should talk about creating an information and threat-sharing plan with private industry that protects trade secrets; develop a centralized process — perhaps through a non-profit organization — for communicating known threats to industry and government agencies;

7. The Government should support research and development of technologies to enhance security; provide the research community with event data to help them create tools and testing models for securing networks.

Detailed Analysis

1. Detailed study and description of the threat landscape should be carried out in line with the approach followed by other countries;

The policy document only gives a brief overview of the various forms of threats which are present in information networks. It does not enumerate the sources as well as the different categories of threats. Towards this, reference may be made to Para 2.1 of the Policy, which only provides a sparse overview of the, “threat landscape”. In this regard, it is beneficial to look at the approaches followed by other countries and later adopt a policy which works both globally as well as locally.

The United Kingdom has published the “Cyber Security Strategy of the United Kingdom ” in June, 2009 which devotes Chapter 2 to the identification of threats.[1] The policy first defines the source of these threats emanating from various persons such as, (a) criminals; (b) terrorists; (c) foreign states. It then proceeds to study the method of these attacks.

The United States has published the National Strategy to Secure Cyberspace[2] in February, 2003 which from page 5 till page 11 identifies various risks to Cyber Security. It also ranks threats under five levels.

The Australian Government has commissioned several studies[3] on the state of Cyber Security pursuant to which it has published a paper on Cyber Security Strategy.[4] These include threat identification and measures to tackle them.

Canada lists the various forms and sources of Cyber threats in its Cyber Security Strategy announced in 2010.[5]It also makes the use of statistics and relevant data to identify the threats and well as to suggest policy responses.

Germany's Cyber Security Strategy mentions threat assessment in the framework which has been drawn up by its Ministry of Interior.[6]

A presentation on the Cyber Security Policy of Japan, made by its National Information Security Centre similarly identifies ten risks through past cyber security incidents as well as the projected risks to information infrastructures [7]

1 Cabinet Office, Cyber Security Strategy of the United Kingdom : safety, security and resilience in cyber space, (June, 2009) available at www.official-documents.gov.uk/document/cm76/7642/7642.pdf

2 Department of Homeland Affairs, National Strategy to Secure Cyberspace (Feb., 2003) available at http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

3 Child Health Promotion Research Centre, Review of Existing Australian and International Cyber-Safety Research (May,
2009) available at
http://www.dbcde.gov.au/__data/assets/pdf_file/0004/119416/ECU_Review_of_existing_Australian_and_internati onal_
cyber-safety_research.pdf

4 Australian Government, Cyber Security Strategy (2009) available at http://bit.ly/i9Ktsl.

5 Minister of Public Safety, *Canada's Cyber Security Strategy* (2010) available at
http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf

6 Federal Ministry of Interior, *Cyber Security Strategy for Germany* (Feb., 2011) available at http://bit.ly/eeR1HJ

7 National Information Security Centre, *Cyber Security Policy of Japan* (Feb. 02, 2011) available at www.cipdubaindu.ae/download/Mitsutaka%20Otsu.pdf

Suggestions

- It is important for the policy to examine the level as well the extent of each threat. Only a comprehensive study which identifies the degree of risks and threats can lead to a beneficial cyber security policy absent a sense of paranoia.
- While examining these threats, they may be classified into distinct threat levels and categories.
- It is suggested that only the threats which threaten Government functions as well as critical network infrastructure may be included in this policy.

2. The focus of the policy should be on critical infrastructure.

Our nation's critical infrastructures include those assets, systems, and functions that are vital to our national security, economic need, or national public health and safety. Critical infrastructures encompass a number of sectors, including many basic necessities of our daily lives, such as food, water, public health, emergency services, energy, transportation, information technology and telecommunications, banking and finance, and postal services and shipping. All of these critical infrastructures increasingly rely on computers and networks for their operations. The policy needs to identify such critical infrastructure and only prescribe guidelines qua private parties when such infrastructure is managed by them.

An overall Cyber Security framework will include:

1. Determining the business requirements for security;
2. Performing risk assessments;
3. Establishing a security policy;
4. Implementing a cyber security solution that includes people, process, and technology to mitigate identified security risks; and

5. Continuously managing security.

Analysis

a) Para 6.3 recommends several measures which include , "use legal software and update at regular intervals". In a country like India, where a very large number of instances of unlicensed software usage have been reported due to high price of proprietary software, it is important for the government to encourage us of Free and Open Source Software whichisverifiable,auditable. Proprietary software, which is mass produced and only provides minimum level of security dependant upon the market demand without much regard to a comprehensive security structure which encompasses concerns of the users as well does not give either the users or the Government any control over its structure and makes it difficult to built in security frameworks.

b) Issues such as content monitoring, data retention, encryption, child safety etc. are ancillary issues which though may be linked to Cyber Security require independent scrutiny and examination. If the policy goes ahead with maintaining references to them, it is advisable that it may be clarified that separate studies and policy documents may be taken out with respect to them.

c) Para 5.1.3 prescribes various measures which can be undertaken for the safe use of IT for children and small & home users.

It states that, "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".

If these concerns qua the vulnerability of children has to be addressed then it needs to be addressed through specific and separate legislations. It is also pertinent to mention that these measures, though may be commendable, fall outside the purview of cyber security. Such measures require independent study and a consultative process of their own.

d) Para 3.3(i)((d) states that, "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 follow-up action against a person or organization involves legal action (either civil or criminal), electronic evidence needs to 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."

This para broadly calls for extensive data retention. Here several issues will need to be examined, including, (a) whether the network service provider may legally create user logs for each user; (b) what types of data and under what circumstances will the network service provider have to store data; (c) can such data be stored even if the user specifically requests its deletion; (d) if yes, what will be the period of retention of such data; (e) if the data is retained then is the retention same for all forms of data; (f) how long may back-ups of data be retained despite the specific request of the user to delete it. These issues have a heavy interplay with privacy regulation and hence, data retention as a concern will require independent scrutiny .

Suggestions

- Since the policy is concerned with national Cyber Security it should identify critical infrastructure and then take actions to protect it . This will usually cover a lot of Government infrastructure and where private players control such infrastructures, the Central Government should only prescribe minimum guidelines which does not interfere immensely with their ability to operate. The Government can take steps to help such private players in their Cyber Security needs, and hence their needs for cyber security technology also the Government can take long-term actions to increase the quality and availability of Cyber Security technologies available in the marketplace.

- Bringing small and medium users like individuals and small and medium enterprises and businesses in the policy ambit may impose excessive regulation and the need to use costly software on them without benefit to Cyber Security. They should be excluded from the policy ambit.

- Independent and detailed study is called for distinct issues such as encryption and data retention involving all effected stakeholders. A policy of forbearance should be adopted with respect to these highly topical subjects in the Cyber Security policy.

3. Software running critical services and infrastructure should be audit-able and verifiable by the Government and capable of "designing in" requisite security measures;

a) Critical services should not be provided on mass market software that is un-auditable by the Government. Software running critical services and infrastructure should be audit-able i.e. capable of being studied, reviewed, audited and if required altered by the Government agencies so that the authorities have a way of knowing vulnerabilities in computer networks running critical infrastructure and seek ways to close security holes. Mass market software may not be able to fulfill the security needs of the Government as it usually provides only what is demanded by the market for users who may not have the same considerations the Government requires. Any software that runs critical infrastructure should be available for the Government to study and modify and capable of "designing in" requisite security measures.

b) Cyber Security requires verifiable software engineering practices. Experience has shown that carefully reviewing program source code is only one aspect of building secure software, once a security-aware design process has completed. Compilers and other elements of the program-building "tool chain" can automatically prevent certain security failures in the software they help manufacture. Such "hardening" tools are a well-established feature of the open source computer programming environment. When Government procures open source software, it can directly verify that the software is built using hardening tools. When government procures proprietary software, which it cannot build or rebuild for itself, it must trust the manufacturers representations concerning the use of hardening technology. But in either case, the policy should specify that Government of India (GoI) requires all software it procures to be provided in a form that uses best available practices for software hardening, and that the provider of the software provide means to verify the hardening construction employed.

c) Mobile Network Governance is increasingly becoming more crucial. As increased device and user mobility dissolve the network perimeter as we know it, the need to have a secure mobile network is imperative. It is said that there are inherent weaknesses in the mobile IP protocol that allow the launch of attacks that are relatively straightforward to mount but hard to detect and thwart. Department of Information Technology (DIT) has launched a draft consultation paper on Mobile Governance Policy Framework which has been prepared by the National e-Governance Division (NeGD) within DIT and the current policy needs to harmonize itself with the governance rules laid out.

4. Open Standards compliance should be a necessary component of a comprehensive national Cyber security policy and not merely to “be encouraged”

The draft policy suggests that compliance with relevant open standards be "encouraged" as part of the effort to make government computer networks, solutions, workstations and devices more secure. In fact, DIT has already called for mandatory open standards http://egovstandards.gov.in/notification/Notification_Policy_on_Open_Standards_-_12Nov10.pdf/view compliance to be used in e-governance applications to ensure sharing of information and seamless interoperability of data across applications. Although the Cyber Security policy mentions the need to encourage open standards, in the light of the policy on open standards, it is imperative that open standards are made mandatory. In the area of information security, proprietary standards with its closed nature could lead to security risks and vendor lock-in and have to be avoided.

More important, however, is the necessary role open standards play in securing Government Information Technology (IT). As the draft policy notes, the most important procurement goal is that IT security be "designed in" rather than "bolted on" what Governments buy and use. Open Standards

compliance means compliance with standards that have been produced in a standards process that maximizes public participation and review of implementation, including open source implementation. Open standards openly developed are far more likely to take security into account throughout the design and definition process than programs or solutions represented by a single, proprietary implementation. For this reason, although open standards compliance is nowhere near sufficient to establish "security designed in," it is in practice a necessary component of such an outcome.

The policy lays emphasis on indigenous Reseach & Development (R&D) as imported IT products could turn out to be a veiled security threat. The problem lies in the fact that equipments and software with proprietary source code do not offer an opportunity for auditing and verifying the source code for any malicious code or security loop holes. The answer to such concerns is to lay emphasis on FOSS based products as it provides an opportunity to verify and audit the underlying source code for any security threat. The Government has already invested in R&D activities in the area of FOSS through institutions like C-DAC, NIC and NRCFOSS. Such research can be effectively utilized in the R&D efforts visualized in the area of Cyber Security. Hence the policy could make a special mention of FOSS in the area of R&D as well as software deployment. As the policy rightly points out, collaboration among nations, the private sector and civil society is important in the matter of Cyber Security and FOSS projects with its inherent collaborative nature provides the ideal platform for this.

5. The policy should determine the role Government should play in the defense of critical infrastructures, while safeguarding privacy and civil liberties;

The policy document is lacking with regard to the various legal safeguards which should be maintained in making a secure cyber environment. These safeguards which are constitutionally mandated fall under the broad heads of the right to privacy and the right to free speech and expression. The policy with its focus on cyber intelligence and vulnerability checks could result in violation of the fundamental rights of speech and expression as well as the right to privacy of the citizens.

a) In this respect **Para 2.4** mentions that there is a need for the, “protection of data while in processing handling, storage & transit and protection of sensitive personal information to
create a necessary environment of trust”.

This paragraph which forms one of the few mentions on the importance of privacy of Internet users, does not mention the importance of regulating the circumstances of acquisition of the users data or sensitive personal information. The acquisition of the data and the sensitive personal information of the user needs to be dealt carefully by the government agencies or any other parties authorized to do so and strict penalties must be imposed on any misuse of such data. Governments all over the world have been concerned about collection of sensitive information such as health records, location based records and services, mining of personal information for commercial purposes. Such activities without proper safeguards could open a plethora of problems .

b) **Para 6.1** and **Para 6.2** contain various actions which should be carried out by Network Service Providers (specifically Internet Service Providers) and by large corporates respectively. One of these action points state that, “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.” These acts, specifically “net traffic monitoring” may involve the monitoring and collection of user logs which may even contain their browsing history. This will result in substantial privacy violations and is against the constitutional mandates of the right to privacy. This is because such general pro-active measures cannot be taken when a person's privacy is involved. Invasion of a person's privacy is allowed under law, only on a case to case basis by issuing a specific order.

Here reference may be made to the Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data of Information) Rules, 2009. The rules clearly contemplate under Rule 3(2), that, “no directions for monitoring and collection of traffic data or information under sub-section (3) of section 69B of the Act shall be issued, except by an order made by the competent authority.” Hence, these rules which are specifically formed to govern “net traffic monitoring”, do not contemplate any, “pro-active measures”, but prescribe passivity for Network Service Providers. This inherent passivity, is only interfered on the basis of a specific order which is issued on the grounds and the procedures which have been prescribed under the Information Technology (Procedure and

Safeguard for Monitoring and Collecting Traffic Data of Information) Rules, 2009. Such orders should reflect the constitutional concern for privacy as emphasized by the Hon'ble Supreme Court in the telephone tapping case. Peoples Union for Civil Liberties v. Union of India (1997) 1 S.C.C. 301. Also, on May 11, 2011 the Hon'be Supreme Court made observations with respect to the right of privacy and responsibility of the network service provider when a request is made by any Government agency to tap telephonic conversations. This was done in the case of Member of the Parliament, Sh. Amar Singh wherein while criticizing Reliance Infocomm for tapping Sh. Singh's phone on the basis of 'forged' documents, the Hon'ble Court observed , "… the service provider has to act as a responsible agency and cannot act on any communication." The Hon'ble Court also asked the government to frame guidelines for the interception of telephone conversations to prevent illegal tapping by service providers. In view of the aforementioned observations by the Hon'ble Court, it is clear that the law of the land requires strict adherence to the fundamental rights enshrined in the Constitution which include the Right to Privacy with respect to both the wired as well as the wireless network.

Maintenance of user logs and the retention of data beyond the purpose for fulfilling the technical function as requested by the user poses a great privacy risk. This becomes incredibly relevant in light of the recent Ratan Tata privacy litigation in the Supreme Court, where the issue is not the legality of the telephone tapping but the unauthorized dissemination of the tapped conversations. Here the periods and the conditions under which data may be retained is important to be chalked out. In this respect the recommendation for independent study of data retention standards and clearer guidelines is restated.

c) **Para 3.3(i)(d)** which states, that electronic records should be protected from "falsification". This may even imply that each electronic record may be matched against an individual user and may lead to legal controls against pseudonymous and anonymous online activity. This may not only endanger privacy but also will have a chilling effect on online free speech and expression.

It is also important that while maintaining a secure environment online, the great potential for free speech inherent in the Internet should not be muzzled. Towards this various references need to be suitably inserted to ensure that content policing and filtration is not carried on by Internet intermediaries in purported compliance with Cyber Security requirements.

d) **Para 6.2** which states that actions by large corporates should "promote acceptable users behavior in the interest of safe computing both within and outside" should be redrafted with deletion of the term, "acceptable behavior".

Similarly, **Para 2.4** which states that there should be a focus on, "creation of a culture of cyber security for responsible user behavior & actions" should be suitably amended. Here it is important that, "responsible user behavior & actions" should not lead to intermediaries blocking access and services to persons utilizing pseudonyms to avail a certain level of online anonymity.

Also, whenever any blocking of information is carried out it should be as per the provisions of the Information Technology Act, 2000. Moreover, it is suggested in cases, when such blocking is ordered through a government authority, such an order should be made publicly available on the Ministry of Information Technology's website.

Hence, it important for the Cyber Security Alert as issued by CERT-in to be detailed as well mention the grounds of opinion why the alert has been issued. It should also mention to whom it applies. In a sense it should clearly mark out the applicable class of Government organizations/service providers, to whom the cyber security alert is most relevant.

6. The Policy exceeds the rule making powers of the Government and seems to legislate beyond the realms permitted under various laws of the land.

The Cyber Security Policy should be careful in going beyond the sources of legal authority existing under the Information Technology Act, 2000. An absence to pay regard to these provisions may lead to a variance from the mechanism prescribed under law.

a) In this respect, reference may be had to**, Para 6.1** which states that actions by network service providers should, "conform to legal obligations and cooperate with law enforcement activities including prompt actions on alert/advisories issued by CERT-in". **Para 3.1 (bullet 4)** states that, "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 24x& basis".

This is contrary to the current state of law as laid out in Sec. 69 of the IT Act and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 formed thereunder. Sec. 69 as well as provisions of the rules do not contemplate for any private agreements to be entered with intermediaries or network service providers. They only allow actions through orders which are issued in specific circumstances.

The policy exceeds this objective in prescribing actions for network service providers, large corporates, small/medium users and home users and by mentioning monitoring and surprise check mechanisms. A policy does not involve law making and hence new restrictions/ requirements apart from those laid out in statutes cannot be incorporated in it.

b) Provisions regarding security practices and procedures to be implemented by organizations that handle sensitive personal data or information are laid out in Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 . The rules require such organizations to implement "security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business" (sic). International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements" is a standard on Information security prescribed by the rules. Intermediaries, including telecom service providers, network service providers, INTERNET service providers, web-hosting service providers, search engines, on-line payment sites, on-line auction sites, online market places and cyber cafes, have to comply with such procedures as per the provisions of Information Technology (Intermediaries guidelines) Rules, 2011 .

This is a statutory requirement that has to be complied by such organizations. The policy, without any statutory basis, cannot require organizations to adopt any procedure beyond those mandated by statutory provisions.

Also if under the Policy, any such restrictions are imposed on organizations (intermediaries, large corporates, small and medium users) as well as regulations of operations should be based on statutory provisions. Such actions cannot be undertaken through clauses in a policy document. CERT has only limited powers under Sec. 70B of the IT Act. The policy mentions cyber security intelligence and conducting of surprise vulnerability checks(Page 9, Para 3.3) but the statute does not seem to provide the legal sanction for such actions.

c) **Para 5.1.3** prescribes various measures which can be undertaken for the safe use of IT for children and small & home users.

It states that, "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"

If these concerns qua the vulnerability of children has to be addressed then it needs to be addressed through specific and separate legislations. It is also pertinent to mention that these measures, though may be commendable, fall outside the purview of cyber security. Such measures require independent study and a consultative process of their own.

7. Cyber Security Policy Needs to Harmonize itself with the other policies released by Department of Information Technology (DIT) or any other departments of the Government of India so as to avoid confusion, duplication, conflict or additional burdening of the stakeholders.

The National Cyber Security Policy while acknowledging different policies and guidelines issued by the government has to ensure harmonization with these policies and guidelines in formulating the security policy.

a) DIT has notified a policy on open standards[10] on November 12, 2010 to be used in e-governance applications to ensure sharing of information and seamless interoperability of data across applications. Although the cyber security policy mentions the need to encourage open standards, in the light of the policy on open standards, it is imperative that open standards are made mandatory.

b) The Department of Information Technology has released guidelines for information security as part of the e-governance standards initiative.[11] The e-Governance Security Assurance Framework categorizes information systems as low, medium and high impact based on potential impact of a security incident. Detailed guidelines have been released by DIT for each category of the system. However, the current policy neither mentions these guidelines nor takes the format into account. The security policy needs to achieve harmony with such

c) The Government has also issued "Guidelines for Indian Government Websites"[12] that has been included in the Central Secretariat Manual of Office Procedure. These guidelines mention security to be adopted in the matter of Government websites. Inclusion of these guidelines in the current cyber security policy would avoid any confusion on the part of those effected duplication of work .

10 http://egovstandards.gov.in/notification/Notification_Policy_on_Open_Standards_-_12Nov10.pdf/view
11 http://egovstandards.gov.in/guidelines/guidelines-for-Information-Security/viewguidelines that have been released by the Government.
12 http://egovstandards.gov.in/guidelines/guidelines-for-Indian-Government-web-sites/view 17

Suggestions

- Free speech and privacy concerns need to be incorporated and substantially highlighted in the policy.
- Policy should be careful in going beyond the sources of legal authority existing under the Information Technology Act, 2000. An absence to pay regard to these provisions may lead to a variance from the mechanism prescribed under law.
- The Cyber Security Policy appears to be dealing with issues which have been dealt by pre-existing provisions of the Information Technology Act, 2000. There is a need to maintain consistency, coherence and harmonization with existing rules.
- Certain issues in the policy fall outside the mandate of CERT, hence it is suggested to have a distinct organization to study these issues.

Annexure-B

BSA GLOBAL CYBERSECURITY FRAMEWORK

Over the last 20 years, consumers, businesses and governments1 around the world have moved online to conduct business, and access and share information. This shift to a digital world has revolutionized personal interactions, education, commerce, government, healthcare, communications, science, entertainment and the arts, etc. It has delivered unprecedented efficiencies, and it will continue to yield immense benefits to our global society.

1 For the purposes of this document, the term "governments" includes the European Union institutions.

However, as opportunities expand, so do the number of risks. Consumers, businesses and governments face a variety of online threats, which can undermine trust in the digital environment – the single greatest platform for commerce and sharing information.

Protecting cyberspace is a shared responsibility. No single entity or group of stakeholders can address the problem alone – and no individual or group is without responsibility for playing a part in cyber security. The technology industry, consumers, businesses and governments must all take steps to secure their own systems and to collaborate with each other to define and implement comprehensive cyber security policies and technologies.

Cyber security is not just about protecting against current threats. It also yields the benefit of enabling greater and more sophisticated uses of the digital environment. Cyber security gives individuals, companies and governments greater confidence that they can operate in this environment and can entrust it with valuable assets and information.

Governments around the world have a multifaceted role to play in cyber security, including:

- Protecting their information systems.
- Working with the private sector to protect the digital infrastructure.
- Investigating, pursuing and prosecuting cybercriminals.

Currently, too few governments are sufficiently policing cyberspace, and few have put in place needed policies to effectively contribute to global cyber security. Significant opportunities exist to work globally and collaboratively to improve cyber security.

No country can address cyber security risks in isolation. The Business Software Alliance (BSA) Global Cyber security Framework is a comprehensive roadmap to build an integrated and functioning global policy response to cyber security.

Guiding Cyber security Principles

To help governments build and implement comprehensive and workable plans that function at the national and global levels, BSA has established the following set of guiding principles:

- **Trust**—cyber security policy should enhance the confidence of consumers, businesses and governments in the confidentiality, integrity and availability of the online environment.
- **Innovation**—cyber security is a fast-paced race, in which we must stay ahead of cybercriminals who adapt constantly. Cyber security policy should maximize the ability of organizations to develop and adopt the widest possible choice of cutting edge cyber security solutions.
- **A risk-based approach**—consumers, businesses and government agencies seek to protect a wide spectrum of targets against a wide variety of cyber threats. Cyber security policy should enable them to implement the security measures that are most appropriate to mitigating the specific risks they face.
- **International standards**—industry-led, internationally accepted standards[2] underpin the global information technology (IT) ecosystem and spur the development and use of innovative and secure technologies. Cyber security policy should preserve the role of international standards.

- **Global policy convergence**—cyber security policy must recognize the borderless nature of the Internet, of the global economy and of cyber threats. As a result, governments should cooperate to ensure their national cyber security policy frameworks integrate with global approaches and practices.

[2] For the purposes of this document, the term "standards" means a specification with the following characteristics:
1. It is developed through an open, consensus-based process;
2. It is publicly available without cost or for a reasonable fee to any interested party;
3. Any patent rights necessary to implement the standard are available to all implementers on reasonable and non-discriminatory (RAND) terms, either with or without payment of a reasonable royalty or fee; and
4. It should be in sufficient detail to enable a complete understanding of its scope and purpose and to enable competing implementations by multiple vendors.

A 12-Point Roadmap for Global Cyber security

To help governments implement the guiding principles listed above, BSA has developed a specific 12-point roadmap to guide policy and enforcement efforts. This roadmap is focused on helping governments develop strong, workable policies to improve cyber security at a national level, while at the same time contributing to, and integrating with, an international framework for global cyber security. This roadmap includes the following key efforts.

Deter and punish cybercrime

1. Governments should enact strong laws against cybercrime:
   - Ratify, and adopt laws to implement, the Council of Europe Cybercrime Convention.
   - Countries that are not ready or able to ratify the Convention should look to alternative resources, such as BSA's model cybercrime law, to modernize and harmonize their domestic laws.
   - Laws need to be regularly updated to address all aspects of modern cybercriminal activity.
   - Laws need to provide deterrent criminal penalties and civil damages.

2. Governments need to make fighting cybercrime a priority by efficiently and effectively enforcing cybercrime laws, including allocating adequate resources to enforce cybercrime laws:

   - Sufficient numbers of dedicated investigators, prosecutors and judges.
   - Law enforcement personnel need to be trained about sophisticated cybercrime.
   - Law enforcement also needs adequate equipment to conduct investigations.

3. Cybercrime rings often span the globe. Law enforcement action must also take place across borders:
   - Law enforcement agencies need to build networks of relationships with their counterparts in other countries and regions.

Adopt a risk-based approach to cyber threats

Consumers, businesses and government agencies seek to protect a wide spectrum of targets against a wide variety of cyber threats. A fundamental principle of effective security protection is that not all targets require the same level of protection, and not all threats present the same risk. Cyber security policy should therefore enable consumers, businesses and government agencies to implement the security measures that are most appropriate to mitigating the specific risk they face.

4. Governments should preserve the contribution of industry-led, internationally accepted standards to global cyber security:
   - These standards not only underpin the global IT ecosystem, but they greatly contribute to cyber security by spurring the development and use of innovative and secure technologies.

- Governments should permit the use of cyber security technologies according to internationally accepted, private sector developed standards, and the use of various solutions and approaches to cyber security.
- Governments should not mandate compliance with country-specific cyber security standards, in particular standards developed by government agencies. Such mandates may cut off their country's access to the most innovative, cost-effective and valuable security technologies offered on the global marketplace, as well as inhibit their domestic industry from competing on equal terms with their foreign competitors. For example, governments should not require or mandate proprietary cryptographic algorithms or artificially limit the strength of encryption, but should accept publicly available, peer-reviewed algorithms.

5. Governments should maintain a policy of technology neutrality when they develop cyber security policies and laws:

- Governments should not prohibit or require the acquisition or deployment of specific products or technologies, including specific hardware or software.
- Technology-neutral policies are fundamental to effective cyber security protection because they ensure that individuals and organizations can deploy the security measures that are necessary to mitigate the specific cyber risks they face.

6. Governments should lead by example in implementing risk-based security measures (people, process and technology) to protect their computers, networks and systems.

7. Governments should partner with industry to develop strategies to strengthen cyber security and privacy through improved use of reliable and risk-based online identity management, authentication and access control solutions:

- Unreliable identity, authentication and access controls are one of the major factors facilitating successful cyber attacks.
- Any strategy to improve the use of reliable electronic identities must respect privacy.
- Greater use of identity, authentication and access controls solutions that offer levels of protection commensurate with risk would protect privacy and foster cyber security.

Inform and protect consumers

8. Governments need to educate the public – home users, children and small businesses in particular – about **—** "cyber hygiene", "safe" and "ethical" computing:

- This includes education about software piracy, because many risks to the public come from the use of pirated software.
- Governments should tap industry resources for such efforts because industry – and the IT industry in particular – have developed a great deal of educational cyber security material, have marketing expertise and have established channels to communicate with the public.

9. If governments are considering whether they should create legal frameworks about data protection and privacy, they should consider whether requirements would be appropriate to protect personally identifiable information against unauthorized access and disclosure. Such data security frameworks should take inspiration from existing best practices, such as:

- How public and private organizations develop, implement, maintain and enforce administrative, technical and physical safeguards of personally identifiable information.
- If such requirements are instituted, they should be reasonable and appropriate to the size and complexity of the entity, the nature and scope of its activities and proportional to the likelihood and severity of the potential harm.

10. If governments are considering whether they should create legal frameworks to require that public and private organizations notify security breaches of sensitive consumer data, they should consider the following recommendations based on existing best practices:

- Limit such breach notification requirements to situations where there is a significant risk of personally identifiable information being used to cause harm.

- Provide that notification is not required if the PII has been rendered unusable, unreadable or indecipherable to an unauthorized third party through the use of practices or methods such as encryption, redaction, access controls and other such mechanisms which are widely accepted as effective industry practices or industry standards.
- Provide for government enforcement and preclude liability to third parties.
- Be flexible enough to take into account the great variety of business arrangements as well as the risks confronted within specific industry or market segments.

Build capacity to prevent and respond to cyber incidents

11. Governments should build capacity to facilitate the sharing of cyber security information among companies and between the government and private sector (e.g. actionable threat information, response plans, etc.) Information sharing can enhance the protection of critical information infrastructure, most of which is owned and operated by the private sector:

- Governments should facilitate this information sharing by supporting the creation of public, private and joint capabilities. This includes both human and technical resources, as well as appropriate legal protections against anti-trust claims, disclosure requirements, etc.
- Governments should promote the development and adoption of industry best practices on information sharing.
- Governments should address any policy or legal barriers that may inhibit information sharing. However, information sharing must be voluntary. Any obligation to share data would run against the need for organizations to comply with incompatible legal requirements (such as privacy laws, wherever they are applicable), and protect their confidential information, that of their customers, trade secrets, their intellectual property, etc.

12. Governments should support cyber security innovation through education and research and development (R&D):

- Governments should support the development and generalization of cyber security curricula in university-level IT education.
- Government support of cyber security R&D helps meet the future technological needs of each country's infrastructure, as well as help each country develops its IT industry.
- Governments should support cyber security R&D through public funding of basic and long term research. They should limit their involvement in applied R&D to circumstances where the technological solution that is sought is not commercially available, and its absence creates a measurable security gap – thus focusing government resources on long-term need.
- Governments should also consider creating incentives that encourage the private sector to conduct cyber security R&D.