

Overview of Cyber Security in India

G.Narendra Nath

Deputy Director General(Security)

Legislation, Policies and License Conditions

- Indian Telegraph Act, 1885
- Indian Wireless Telegraphy Act, 1933
- Information Technology Act, 2000
- National Telecom Policy, 2012
- National Cyber Security Policy, 2013
- Security related license amendment to Telecom Service Provider (TSP) licenses in May/June 2011

National Telecom Policy, 2012

- Mandate and enforce that the Telecom Service Providers take adequate measures to ensure the security of the communication flowing through their network by adopting contemporary information security standards

National Telecom Policy, 2012

- Communication assistance to Law Enforcement Agencies (LEAs)
 - Regulatory measures
 - Telegraph Act
 - License conditions
 - Individual privacy
 - Follow International practices
 - Develop and deploy State of art system

National Telecom Policy, 2012

- Create an institutional framework through regulatory measures to ensure that safe-to-connect devices are inducted into the Telecom Network and service providers take measures for ensuring the security of the network.

National Telecom Policy, 2012

- Build national capacity in all areas – specifically
 - Security standards
 - Security testing
 - Interception and monitoring capabilities
 - Manufacturing of critical telecom equipment - that impinges on Telecom network security
 - Communication assistance for law enforcement.

National Telecom Policy, 2012

- Mandate standards in the areas of functional requirements, safety and security and in all possible building blocks of the communication network i.e. devices, elements, components, physical infrastructure like towers, buildings etc.
- Develop a rational criterion for sharing of costs beyond a threshold limit between Government and the service providers in implementing security measures.

National Telecom Policy, 2012

- Mandate testing and certification of all telecom products for conformance, performance, interoperability, health, safety, security, EMF/EMI/EMC, etc. to ensure safe-to-connect and seamless functioning in the existing and future networks.

National Telecom Policy, 2012

- To create suitable testing infrastructure for carrying out conformance testing, certification and to aid in development of new products and services. These state-of-the-art labs/infrastructure would be suitably positioned to make them available to engineering/academic institutions to assist the scholars in telecom product development

National Telecom Policy, 2012

- To endeavor to make available Global Mobile Personal Communication by Satellite (GMPCS) compliant with security requirements
- To facilitate establishment of a National Mobile Property Registry for addressing security, theft and other concerns including reprogramming of mobile handsets

National Telecom Policy, 2012

- A Unique Identity (AADHAR) based electronic authentication framework would be integral part of providing service to the people, - financial inclusion, direct benefit transfer and many more.
- eKYC
 - Proof of Identity
 - Proof of Residence

National Cyber Security Policy 2013

- Aims to create a cyber security framework, leading to specific actions and programmes to enhance cyber security posture
- Integrated vision and a set of sustained and coordinated strategies for implementation
- Enable individual sectors and organizations in designing appropriate cyber security policies to suit their needs

National Cyber Security Policy 2013

- Assurance framework through compliance to global security standards and best practices by way of conformity assessment of product, process, technology and people.
- National and sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure.
- Operating a 24 x 7 NCIIPC and mandating security practices related to the design, acquisition, development, use and operation of information resources.
- Create a workforce of 500,000 professionals in 5 years.

National Cyber Security Policy 2013

- Establishing infrastructure for testing and validation of security of ICT products
- Create a culture of cyber security and privacy through effective communication and promotion.
- Develop effective public private partnerships and collaborative engagements
- Enhance global cooperation

National Cyber Security Policy 2013

- National nodal agency, - CERT-In
 - Sectoral CERTs
 - CMP
 - Cyber security drills
- All organizations
 - CISO
 - Information Security Policies
 - Specific budgets
- Open Standards
 - Use of open standards
 - Consortium of Government and private sector for availability of tested and certified IT products based on open standards

National Cyber Security Policy 2013

- For CII
 - 24 x 7 NCIIPC
 - Use of validated and certified IT products
 - Security Audit
 - Certification of all security roles
 - Secure application/software development process

National Cyber Security Policy 2013

- Supply chain risks
 - Testing infrastructure
 - Trusted relationships
 - Create awareness of threats etc.

- National Cyber Coordination Centre, - a multi stake holder body. Obtain and study patterns in meta data and share information with stakeholders for ensuring cyber security.
- Centralised Monitoring System, - for automation of lawful Interception. Ensure national security through use of cyber space. Address issues of privacy, confidentiality

Security Related Licence Amendment

- Security Related Amendment to Telecom Service Provider license in May/June 2011
 - Universal Access Service Licence
 - National Long Distance and International Long Distance Licence
 - Internet Service Provider(without Internet Telephony) Licence
 - Internet Service provider(with Internet Telephony) Licence
- Provisions part of new Unified License regime introduced in 2013

- **Requirement-1:**

- The licensee shall have organizational policy on security and security management of their networks. They should submit their policy to the licensor.

- **Requirement-2:**

- The following should be part of the policy:
 - Network Forensics
 - Network Hardening
 - Network Penetration test
 - Risk assessment
- Actions to fix problems and to prevent such problems from reoccurring etc
- Should take all measures in respect of these activities.

- **Requirement-3:**

- The licensees shall audit their network from security point of view once in a financial year

- Or

- Get their network audited from security point of view by an agency which is certified to carry out audit as per ISO 15408 and ISO 27001.

- **Requirement-4:**
 - Licensee shall induct only those network elements into his telecom network, which have been got tested as per relevant contemporary Indian or International Security standards from any international agency/labs of the standards.

- Where third party testing is not available, testing can be done by an independent setup within organization. In such cases certificate to be provided stating that -
 - No third party lab exist which test the equipment as per relevant security standards
 - The equipment has been tested by an independent setup within organization as per relevant security standards
- The copies of the test results and test certificates shall be kept by the licensees for a period of 10 years from the date of procurement of the equipment

- **Requirement-5:**
 - The licensee shall Include all contemporary security related features as prescribed under relevant security standards while procuring equipment
- **Requirement-6:**
 - Implement all such contemporary features into the network
- **Requirement-7:**
 - Keep a list of features, equipment, software etc procured and implemented till they are in use
- **Requirement-8:**
 - The same may be subjected to inspection and testing by licensor in the network or otherwise

- **Requirement-9:**

- The licensee shall employ only-

- Resident
 - Trained
 - Indian nationals

- **As**

- Chief Technical Officer/s
 - Chief Information Security Officer
 - Nodal Officers for handling interception and monitoring cases
 - In-charge of:
 - GMSC, MSC, Softswitch, Central database
 - System Administrator/s

- **Requirement-10:**

- The licensee shall ensure all the documentation including software details are obtained from manufacturer/vendor/supplier in English language

- **Requirement-11:**

- The licensee shall keep a record of operation and maintenance procedure in the form of a manual

- **Requirement-12:**

- The licensee shall keep a record of all operation and command logs

- For a period of 12 months

- Same information shall be stored/retained for 24 months in a non-online mode

- Command logs shall include

- Actual command given

- Who gave the command

- When the command was given,- with date and time

- From where the command was given

- **Requirement-13:**
 - The licensee shall keep a list of user ID linked with name and other details of the user duly certified by the system administrator
- **Requirement-14:**
 - The licensee shall keep a record of all software updates and changes
 - Major updates and changes should be informed to licensor within 15 days of completion of such updates and changes
- **Requirement-15:**
 - The licensee shall keep a record of supply chain of the products (hardware/software). This should be taken from the manufacturer/vendor/supplier at the time of procurement of the products.

- **Requirement-16:**
 - Comply with the conditions of the Remote Access(RA)
- **Requirement-17:**
 - The licensee shall Create facilities for monitoring all intrusions, attacks and frauds within 12 months of issue of the amendment and report the creation when done so to licensor
- **Requirement-18:**
 - Report on intrusions, attacks and frauds to
 - Licensor
 - CERT-IN

- **Requirement-19:**

- Suitable agreement clauses with vendor as follow:
 - To ensure that TSP, Licensor/DOT and/or its designated agencies to inspect the
 - hardware
 - software
 - design
 - development
 - manufacturing facility
 - supply chain
- To subject all software to a security/threat check any time during supplies of equipment
- Number of visits will be limited to two in a purchase order
- For order valuing more than Rs.50 crore expenditure upto 40 man-days shall be borne by the licensee directly or through vendor

- **Requirement-20:**

- Licensee shall provide location details of specified mobile customers in the license service area
- Location details should be part of CDR in the form of latitude and longitude, besides the co-ordinate of the cell sites.
- These details will be provided for specified mobile numbers. Within a period of three years location details shall be part of CDR for all mobile calls

- Suggested steps in Annexure to amendment letter:
 - Agreement with hardware/software manufacturer/vendors and/or suppliers
 - Safe to connect
 - Checked for risks and vulnerabilities
 - Service continuity and service up-gradation
 - Create a forum say,- Telecom Security Council of India
 - To increase security assurance levels
 - Share common issues
 - Build own capability and capacity to maintain and operate the network

Remote Access

- Requirements of Remote access to the network
 - Online mirror image
 - Audit trail
- Mirror image of remote access information for monitoring by designated security agencies/licensor
- Complete audit trail of remote access activities to be maintained for six months. After six months RA logs to be stored offline for a further one year

- Conditions to be satisfied:
 - Provided only to approved locations abroad through approved locations in India
 - Provide IP addresses of foreign and Indian locations
 - Through secure connections
 - List of commands and their functions to be submitted to respective TERM cell and make them aware

- Install local RA storage server and store RA command logs locally
- Uptime to be 99.99%, shutdown/mtce with prior intimation to respective TERM cell
- Capability to restrict RA access
- Audit trail for each and every approved location in India
- Mirror image may be available at centralised location for monitoring
- RA not to be enabled for access to LIS, LIM, call contents and such sensitive sector/data
- Capability to search on key words or commands