Conference of State IT Ministers and IT Secretaries

Cyber Security & Cyber Law

13.2.2018

Ministry of Electronics and IT
Government of India

National Cyber Security Policy

Framed by MeitY in 2013

Vision

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

Mission

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

National Cyber Security Policy Strategies

i. Creating a secure cyber ecosystem
ii. Creating an assurance framework
iii. Encouraging Open Standards
iv. Strengthening the Regulatory framework
v. Creating mechanisms for security threat early warning, vulnerability management and response to security threats
vi. Securing E-Governance services
vii. Protection and resilience of Critical Information Infrastructure
viii. Promotion of Research & Development in cyber security
ix. Reducing supply chain risks
x. Human Resource Development
xi. Creating Cyber Security Awareness
xii. Developing effective Public Private Partnerships
xiii. Information sharing and cooperation
xiv. Prioritized approach for implementation

Information Technology Act, 2000

- Enacted on 17th May 2000 and further amended as The Information Technology (Amendment) Act, 2008 was enforced on 27th October 2009
- To provide legal recognition for transactions:-
  - Carried out by means of electronic data interchange, and other means of electronic communication, commonly referred to as "electronic commerce“
  - To facilitate electronic filing of documents with Government agencies and E-Payments
  - To amend the Indian Penal Code, Indian Evidence Act,1872, the Banker’s Books Evidence Act 1891,Reserve Bank of India Act ,1934
- Computer crimes in the Act are classified into two categories :
  - Civil offences
  - Criminal offences

Role of State Government in IT Act

- Data protection (Section 43A) – Body corporate liable to pay compensation for sensitive personal information leakage
  - u/s 46, 47: Appointment of Adjudicating Officer for holding inquiries under the Act
  - **State IT Secretaries have been notified to be the Adjudicating Officer.**

- u/s 69A Rule - Procedure and Safeguards for Blocking for Access of Information by Public
  - **Nodal officers** nominated from **Ministries/Depts. and States** to forward request for blocking
- u/s 69 Rule - Procedure and Safeguards for Interception, Monitoring and Decryption of Information
  - Union Home Secretary and **Home Secretaries of States/UTs** empowered to issue direction
- Intermediaries guidelines rules, 2011
  - Section 79(3)(b) being read down to mean that an intermediary upon receiving actual knowledge from a court order or on being notified by the **appropriate government or its agency** that unlawful acts relatable to Article 19(2) are going to be committed then fails to expeditiously remove or disable access to such material.
- u/s 79A Scheme for Notifying Examiner of Electronic Evidence
  - Any Department, body or agency of the Central Government or a **State Government** seeking to be notified as an Examiner of Electronic Evidence can apply to MeitY

Chief Information Security Officer (CISO)

- MeitY has issued direction to all State/UT Governments and all Central Government Ministries/Departments & Critical Sector Organizations to appoint CISO
  - To report directly to Secretary/CEOs in PSUs
  - Roles and responsibilities of CISOs prescribed in March 2017.
  - CISO Roles and Responsibility are available at MeitY website http://meity.gov.in/writereaddata/files/CISO_Roles_Responsibilities.pdf

INDIAN COMPUTER EMERGENCY RESPONSE TEAM
Ministry of Electronics and IT
Government of India

No. [illegible] Dated: [illegible]

Ref: Ministry of Electronics and IT letter No. [illegible]

Sub: Key Roles and Responsibilities of Chief Information Security Officers (CISOs) in Ministries/Departments and Organisations managing ICT operations

1. CISO to be appointed in each Ministry/Department/Organisation

1.1 [illegible]

(a) [illegible]

(b) [illegible]

(c) [illegible]

1.2 [illegible]

[illegible]

- CISO Appointed
  - 23 State Governments/UTs
  - 57 Central Government Ministries /Departments

Cyber Crisis Management Plan (CCMP)

- MeitY has developed and shared CCMP with all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors
    - To deal with with cyber related incidents
        - by rapid identification,
        - information exchange,
        - swift response and remedial actions
        - to mitigate and recover from malicious cyber related incidents impacting critical national processes and Government sector organizations.
    - Plan is updated annually and circulated to all key Central Govt. Ministries/Departments and States/UTs
    - 15 workshops conducted for Ministries/Depts., 9 workshops conducted at State Govt./UTs, 18 Workshops in critical sectors
    - 19 Ministries/Depts., 11 State Govts./UTs and 29 attached offices (critical sector organisations) under Ministries/Depts. developed CCMP

Cyber Surakshit Bharat

- The Cyber Surakshit Bharat programme was launched to educate & enable the Chief Information Security Officers (CISO) & broader IT community to address the challenges of cyber security in partnership with Industry consortium

- The programme was launched on 19th Jan 2018 by Hon'ble MoS(E&IT)

- Training will be conducted in 6 cities starting from April 2018
- Detail content and training calendar is being worked out with Industry consortium
- Details are available at http://negd.gov.in/cyber-surakshit-bharat-programme

Policy Level Interventions

- Guidelines for Secure Application development Issued in June 2017

General Guidelines for Secure Application and Infrastructure

- MeitY has provided awareness material with list of cyber security tools (for dissemination to autonomous bodies like UGC, AICTE and IITs etc. for their students) to M D

Cyber Threats/Attacks Preventive Tools
and
Awareness

- MeitY has directed all Central Government Ministries/Departments, State Government/UTs and Critical Sector to earmark 10 % of Annual IT budget to implement Cyber Security

Public Procurement (Preference to Make in India) Order

- Department of Industrial Policy & Promotion (DIPP) had issued an order on regarding Public Procurement (Preference to Make in India) Order 2017 for encouraging “Make in India” and promoting indigenous manufacturing of goods and services in the country
  - For sector having sufficient local capacity and competition, in procurement value upto Rs 50 lakh only local supplier will be eligible
  - For procurement value above Rs 50 lakh, if L1 bidder is not local supplier, 50% of the order will be L1 bidder and remaining 50% will be given to local supplier provided he matches L1 price
- In furtherance to above order of DIPP, a notification was drafted for Cyber Security products.
  - A company incorporated and registered in India as governed by the applicable Act (Companies Act, LLP Act, Partnership Act etc.) would be entitled to get benefit of the notification.
  - Revenue from the product to be claimed under notification, in the Indian geography and revenue from Intellectual Property (IP) licensing should accrue to the company registered in India
  - The entity claiming benefits under the Public Procurement Order 2017 in addition to being an Indian registered / incorporated entity, and supplying products should satisfy the conditions of IP ownership
  - IP Ownership rights would need to be substantiated by adequate proof, such as adequate documentation evidencing. ownership etc
- The Notification is in the process of approval

Grand Challenge

- To promote domestic Cyber Security industry, MeitY is working on a proposal of Grand Challenge for Start-ups to develop a Cyber security product on a given problem statement
- Start-ups will submit their proposal on the given problem
- Proposals received will be evaluated by a Jury and top 10 proposals will be given support to start develop the product
- There will be two stage review
- Winner will be given prize money of Rs 2.5 crore and two runner-ups will be given Rs 75 lakh each
- The proposal on Grand Challenge from Data Security Council of India (DSCI) is under process in the Ministry

Cyber Security R&D

- Research and development is carried out in the thrust areas of cyber security including (a) Cryptography and cryptanalysis, (b) Network & System Security, (c) Monitoring & Forensics and (d) Vulnerability Remediation & Assurance through sponsored projects at recognized R&D organizations.
    - Social Media Analytics Tool with IIIT Delhi: 47 installations with LEAs in 30 states
    - 10 different Cyber Forensic tools by CDAC Trivandrum: More than 3,500 licenses deployed in LEAs & Forensic labs
    - Honeypots technology by CDAC Mohali to sink malicious traffic deployed
    - Secure mobile communication for Voice & SMS by ECIL & CDAC Hyderabad underway
        - Pilot deployment for 86 senior government officers done.
    - Early warning system to detect Botnets and other malware threats by Amrita University. Deployed in NCCC.
    - Framework for management of Cyber Security technologies developed in July 2017

Capacity Building

Training and Participation

- Under **ISEA Project Phase 1**, more than 44000 candidates were trained in formal / non-formal courses in Information security through 52 institutions
- **ISEA Project Phase 2**, aims to train 1.14 lakh persons in various formal / non-formal courses and more than 13000 Govt. officials by March 2020
- **Participating institutions**: IISc. Bangalore, TIFR Mumbai, 4 IITs, 15 NITs, 4 IIITs, 7 Govt. Engineering Colleges and select centres of CDAC / NIELIT
- **School level**: To be included in CBSE/High School and Plus Two levels
  - Need to develop courseware and take up with CBSE/States
- **User level**: Awareness and communication plan:
- **Technical level**: Certificate programmes, B Tech courses, M Tech courses, PhDs
- **07 new Electronics and ICT Academic Inst. set up**, ~**3000 faculties trained**. New technologies: Cloud, IoT, Encryption, Block chain, Social media, DNS
- Need of Cyber security trained persons estimated 5 to 10 lakhs

Sectoral CERTs

- To deal with increasing Cyber incidence, Sectoral CERTs are to be set-up
- Industry vertical (Finance, Power and Telecom etc.) and State CERTs are to be part of Sectoral CERTs
- CERT-In will be mother of Sectoral CERTs
- Rules already circulated

Standards and Testing

- **Common Criteria Testing Infrastructure**.
  - STQC: Testing as per Common Criteria Standards (ISO 15408) being done at Kolkata, Delhi and Bengluru
  - Private Labs: STQC is in discussion with two labs for empanelment at CC labs

- **Digital Payments Security**
  - Standards for mobile digital payment devices and Instruments: As per the recommendation of the Chandra Babu Naidu Committee on Digital Payments Security, a high Level Committee underthe Chairmanship of Secretary MeitY and DoT was constituted in April 2017. The committee setup two Sub-Committees on Digital Payemts Processes and Technology under the chairmanship of RBI and DoT respectively. Two Sub-Committees have submitted their reports on Standards and Recommendations. The High Level Committee will examine the Report before putting up to the Government of India.

- **IoT Security**
  - Working Groups constituted with Industry to recommend cyber security standards for IoT in Smart transport, Smart Healthcare, Smart Surveillance & Buildings, Smart Manufacturing, Cloud IoT Security & Smart Grid and Energy

- **Significant Strengthening of STQC**
  - Project for strengthening of STQC labs for complete security testing
    - Mobile Phone
    - Conditional Access System (CAS)
    - IoT Devices
    - L0, L1 Biometric devices
  - R&D project for unstated vulnerabilities approved by MeitY

THANK YOU