



Cyber Security standards

Dr.Y.L.P.Rao

Deputy Director General,
Unique Identification Authority of India, New Delhi

Cyber Security Standards

- The need for strategic approach
- Actions to secure cyber space
- Identified initiatives
- Role of Government

The need for strategic approach

- Preventing cyber attacks against the country's critical infrastructures
- Reduce national vulnerability to cyber attacks
- Minimize damage and recovery time from cyber attacks

Actions to secure cyber space

- Forensics and attack attribution
- Protection of networks and systems critical to national security
- Early watch and warnings
- Protection against organized attacks capable of inflicting debilitating damage to the economy
- research and technology development that will enable the critical infrastructure organizations to secure their IT assets

Identified initiatives

- Security Policy, Compliance and Assurance
- Security Incident - Early Warning & Response
- Security training - skills/competence development & user end awareness.
- Security R&D for Securing the Infrastructure, meeting the domain specific needs and enabling technologies
- Security - Promotion & Publicity

Security Policy, Compliance and Assurance

- **Critical Information Infrastructure Protection**
- **Cyber Security Assurance Framework**
- **Trusted company certification**

Security Incident - Early Warning & Response

- **The essential actions under National Cyber Alert System**
- **Creation and Augmentation of Response Capabilities**
- **International cooperation and information sharing**

Security Training - Security, Digital Evidence & Forensics

- *A baseline for IT Security awareness*
 - *Skill & Competence development*
 - *Advanced Manpower Certification programmes*
 - Promote a comprehensive national awareness program
 - Foster adequate training and education programs to support the Nation's cyber security needs
 - Increase the efficiency of existing cyber security training programs and devise domain specific training programs (ex: Law Enforcement, Judiciary, E-Governance etc)
- Promote private-sector support for well-coordinated, widely recognized professional cyber security certifications.

Security R&D

- *Facilitating Basic research, Technology demonstration and Proof-of concept and R&D test bed projects*
- Besides in-house R&D, this sector may find it attractive to undertake collaborative R&D with leading research organizations.

Role of Government

- The deliberations of the National Information Board (NIB), National Security Council (NSC) have stressed the importance of a national strategy on cyber security, development of national capabilities for ensuring adequate protection of critical information infrastructures including rapid response and remediation to security incidents, long term investments in infrastructure facilities, capacity building and R&D. Governments responsibilities in long-term investment and fundamental research will enable development of new concepts, technologies, infrastructure prototypes, and trained personnel needed to spur on next-generation security solutions
- Public-private partnership is a key component of Cyber Security Strategy



- Thank you