

# Mobile Security

(Security: Cyber, Telecom, Cloud)

14<sup>th</sup> March 2014

(Time: 10.00 -12.00 hrs session )

Ram Narain

DDG (Security)

Email.ddgsecurity-dot@nic.in

# 10 Principles

- Practical
- Responsibility
- Involvement
- National Capacity
- Cost Effective
- International Cooperation
- Progressive
- Law of the Land
- Enforcement
- Security

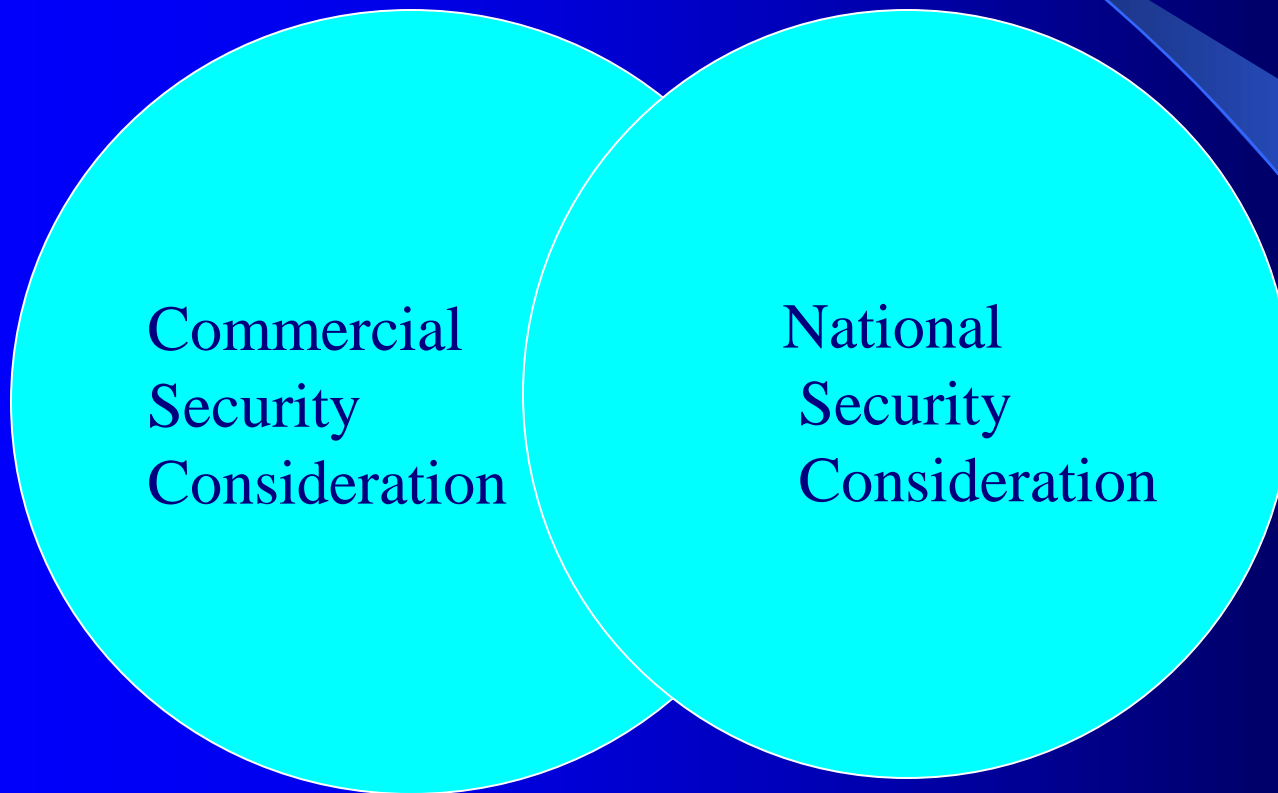
# Important Stipulations

- Telecom service providers to have security policy
- Induct security certified network elements into the network
- Get or carry out a security audit of the network every year.
- Have contemporary security features in the elements and network.
- Keep a records of the software updates
- Maintain maintenance and operation manuals.
- Install intrusion, fraud, attack detections systems and report such incidences to DOT and CERT-In.
- Keep a record of supply of products-hardware and software.

# Perplexities

- Process based testing and individual product testing
- Commercial security considerations and national security consideration.
- ‘You must trust’ and ‘ I have trust’
- Having trust and validating the trust

# Commercial Security Consideration and National Security Consideration



Commercial  
Security  
Consideration

National  
Security  
Consideration

# Network Elements Security Issues

- Non-implementation of security features and protocols.
- Absence of security features and protocols
- Known vulnerabilities
- Un-known vulnerabilities
- Existence of Malware

# Certification Process

- A center to create system, processes and systems for security testing and certification of telecom equipment.
- The center to accredit the testing and certification labs in private, joint or public sector.
- Labs to follow the uniform process for testing and certification as prescribed by the Center.
- Labs to work on commercial basis
- Leverage is to be taken of international standards and testing by third party labs/vendors.
- Work in close coordination with International bodies working in the area of telecom security.

# Expectations from International Standards Bodies

- List of security features and protocols for each element and applicable standard
- Testing, environment, process and test configuration
- Criterion for acceptance
- Dealing with software upgrades and releases
- Body for Maintenance of VAPT data base for Telecom equipment
- Generic tool specification for feature and protocol testing, VAPT and if possible for malware testing
- Mechanism of accepting the feedback and addressing the security issues
- Formulate telecom network security audit standards.



# Security and Robustness of Internet

- Internet Architecture versus Telecom architecture - Can we think of a slightly different network topology of Internet as boundary will get obliterated with NGN, IMS, 5G etc?
- Internet routing versus Telecom routing - trail of communication flowing through the network
- Internet number plan versus Telecom number plan - Maintaining the integrity of identity of the communication originator and terminator.
- Rational distribution of Internet resources
- RA standards

# Outcome

- Harnessing the strengths of process based testing and individual product testing.
- Achieving commercial and national security without duplication of efforts.
- Secured telecom and Internet Networks
- Secure communication, information and data
- Enhanced international cooperation

That is how we would move from ‘Must have trust’ to ‘I have trust’ with option of validating the trust.

**Thanks**