FCC Meeting

Mark Adams,
Director and Chief Architect
Northrop Grumman Information Systems

May 5, 2011

Mark pages according to the proprietary level of information as described in Company Procedure J103 (or remove)

Key Issues

Three issues that are critical to the long-term success of the national public safety broadband wireless network

1. A Nationwide “Security and Identity Management “ strategy

2. A Nationwide “Common Network Applications” Platform

3. A Nationwide “Certification, Validation, and Verification Strategy

There are multiple ways to accomplished reaching the Nationwide goal of building a single operable network however, it will require a *“common owner with authority”* over these Nationwide components.

Mark pages according to the proprietary level of information as described in Company Procedure J103 (or remove)

Network Security

NORTHROP GRUMMAN

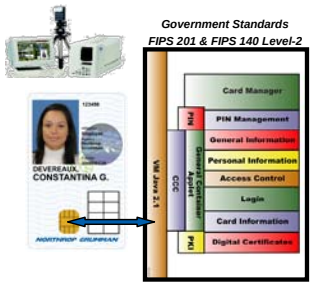
- A fully integrated end-to-end approach to security is required
  - Device, air-interface, backhaul, core network, public safety enterprise networks
- Use of open global standards increases vulnerability to cyber attacks
  - Increasing number and sophistication of cyber attacks on IP-based Internet
- Commission's tentative conclusion protects only the radio-link
  - No requirement to deploy LTE's network domain, user domain, or application domain security
  - Security gaps exist even on the radio-link – LTE doesn't protect user-data integrity
- Security requirements outside of LTE's scope but critical to emergency communications
  - User authentication, physical security of network assets, user device data protection
  - Adherence to agency-specific security policies and procedures
  - Contingency and risk mitigation, Network Availability (SLA Management)
- Additional requirements for possible federal use of the network
  - FIPS 140-2 compliance
  - Network credentialing and certification (HSPD-12)

Public safety broadband network would be an integral part of the national critical infrastructure. It must be protected with the same heightened level of security as any other critical infrastructure assets.

Mark pages according to the proprietary level of information as described in Company Procedure J103 (or remove)

Network User Identity Management

- Network security and User identity authentication are closely linked
  - The Commission treats Network security separately from Roaming Authentication
  - An unauthenticated user on the network is a serious security breach
  - Access to individual agency information will require proper “authentication” no matter where the user resides in the system



- LTE’s authentication framework is user device based
  - SIM card resides in the device and stores user information needed for authentication
  - Need to augment with mechanisms such as multi-factor authentication

- Standard Framework needed for Agency Interfaces
  - Each existing agency has legacy network components which they will want to connect the applications to the Nationwide 700 MHz network
  - Cost efficiency and security will depend on a repeatable and verifiable processes

- Need for a fail-safe, scalable, and robust National Platform for Roaming user authentication
  - Pair-wise roaming agreements between jurisdictions is not a scalable approach
  - Commission recommends a “Clearing House” approach to handle roaming
  - Northrop Grumman “Identity Management” approach builds on the Commission’s concept
    - View all the individual jurisdictional networks as a single logical entity – a “network of networks” or “a single public safety enterprise”
    - All users authenticated by a single “Identity Management” function
    - Common format for essential user information – credentials, role, access level to ensure interoperability across network

Mark pages according to the proprietary level of information as described in Company Procedure J103 (or remove)

Network Applications Platform

NORTHROP GRUMMAN

- True interoperability requires interoperability across all layers – physical, network , and application

- Mandating LTE standards achieves physical and network layer interoperability

- Application layer interoperability requires consideration of QoS, access, security ad priority of service as well as governance and policy issues
  - Unresolved technical issue: QoS over FIPS encrypted tunnels

- Northrop Grumman concurs with the Commission's conclusion of five basic applications that must be supported by all public safety networks
  - 1) Internet access 2)VPN access 3)status homepage 4) network access for ICS users 5) field based server applications

- Northrop Grumman also supports the view that jurisdictions should be free to deploy applications that best meets their needs

Mark pages according to the proprietary level of information as described in Company Procedure J103 (or remove)

Network Applications

- Internet Access
  - Exposes private public safety networks to multitude of cyber attacks on a global scale
  - Proactively monitor and tightly control Internet access to avert malicious threats
  - Leverage industry experience in building, managing, and operating secure IP networks
  - Northrop Grumman recommends centralized access through a Gateway for monitoring and forensics of cyber-activity
- Remote Access Virtual Private Network
  - Needed for secure access to public safety network from external networks e.g. Internet
  - May also be required for inter-jurisdictional roaming
  - Also serve as a tool to provide end-to-end secure connection
  - Northrop Grumman recommends against the use of clientless VPN solutions due to their vulnerability to web-based attacks
  - Northrop Grumman recommends choice of VPN protocols be left to jurisdictions
- LMR Gateways
  - Standards and technologies for voice on LTE still evolving – ecosystem needs development
  - LMR networks still required for mission-critical voice – high cost of investment remains
  - Need for broadband and LMR networks to coexist and interoperate
  - Technologies in place and under development for LMR and broadband interoperability using LMR gateways
  - Northrop Grumman concurs with the use of LMR Gateways for the short term – investment needs to start now
- User Applications
  - Interoperability issues arising due to implementation, operating system,, or client server interfaces
  - Common applications should be provided by the Nationwide “entity” – Public Safety APP STORE
  - Continued dialog with application, vendors and public safety organizations to ensure application interoperability

Mark pages according to the proprietary level of information as described in Company Procedure J103 (or remove)

Network Certification, Validation, and Verification

NORTHROP GRUMMAN

- Coverage and throughput requirements required to achieve operability, spectrum efficiency and interoperability
  - However, performance testing and measurement methodologies vary widely amongst different OEM platforms
  - Northrop Grumman recommends standard methodologies for network validation and verification tests for uniform user experience across all regional networks
- Northrop Grumman agrees with the FCC mandated vendor specific tests conducted within the PTCRB and GCF certification laboratories for interoperability of LTE network element interfaces
  - PTCRB and GCF conformance tests provide validation of only "micro" level interoperability for LTE UE devices and network equipment
- Northrop Grumman recommends additional testing on the live network to capture typical performance metrics such as cell-edge throughput, coverage availability, handoff success rate, call quality etc. to enable "*macro-level"* interoperability
  - Macro level interoperability based on real-world networks performance is the most effective IOT, verification and validation of the NPSTC performance requirements for 700 MHz public safety broadband network
- Northrop Grumman also recommends establishing benchmarks and methodologies for other mission-impacting performance metrics that include:
  - Field integration testing, Performance (stress) testing, Reliability/Redundancy testing, Security testing & certification and Application interoperability testing are necessary IOT components that will enable truly interoperable PS Broadband Network
- Security certification process and a proper *certification authority* needs to be selected so that each jurisdiction doesn't have to have separate processes and requirements

Mark pages according to the proprietary level of information as described in Company Procedure J103 (or remove)