APCO International
Leaders in Public Safety Communications™

HARRIS
assuredcommunications®

# Emerging Technology Forum
# CYBER SECURITY: PERILS AND OPPORTUNITIES

Dr. Dennis Martinez
CTO - Harris RF Communications Division

**June 25, 2013**

# Cyber Security Addresses Two Key Objectives

**Protect Information and Identities from Compromise**

- Based on Ciphering Technology
- Encrypt content and control

**Protect the Network from Attacks that Impact Operations**

- Denial of Service
- Spoofing
- Many other threat types

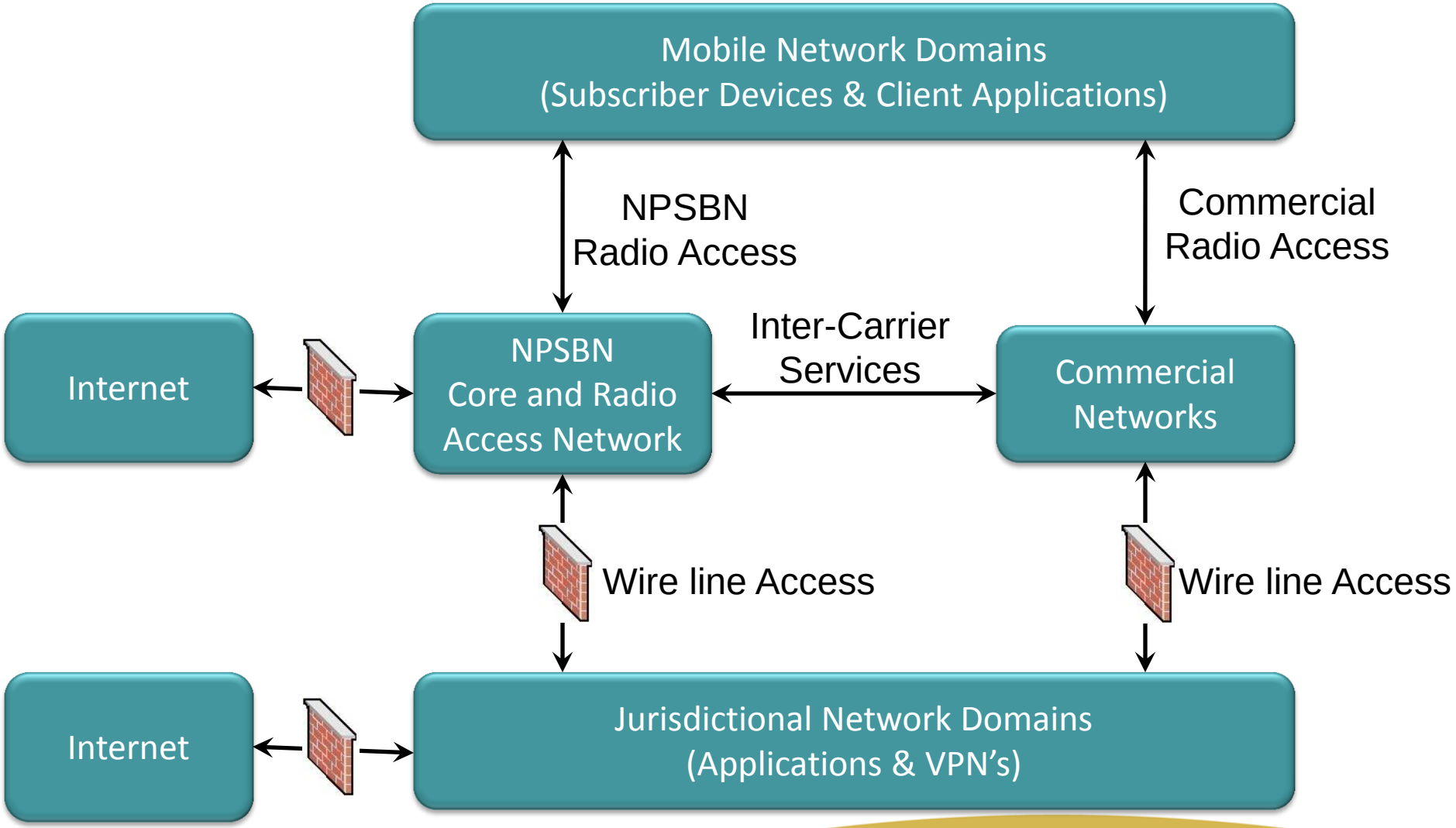
# Cyber Security in the National Public Safety Broadband Network (NPSBN)

- The NPSBN is unprecedented
  - Built on commercial technology
  - Purpose-built for public safety communications
  - Nationwide-service – Millions of users
  - Large eco-system of product/technology suppliers with significant “off-shore content”

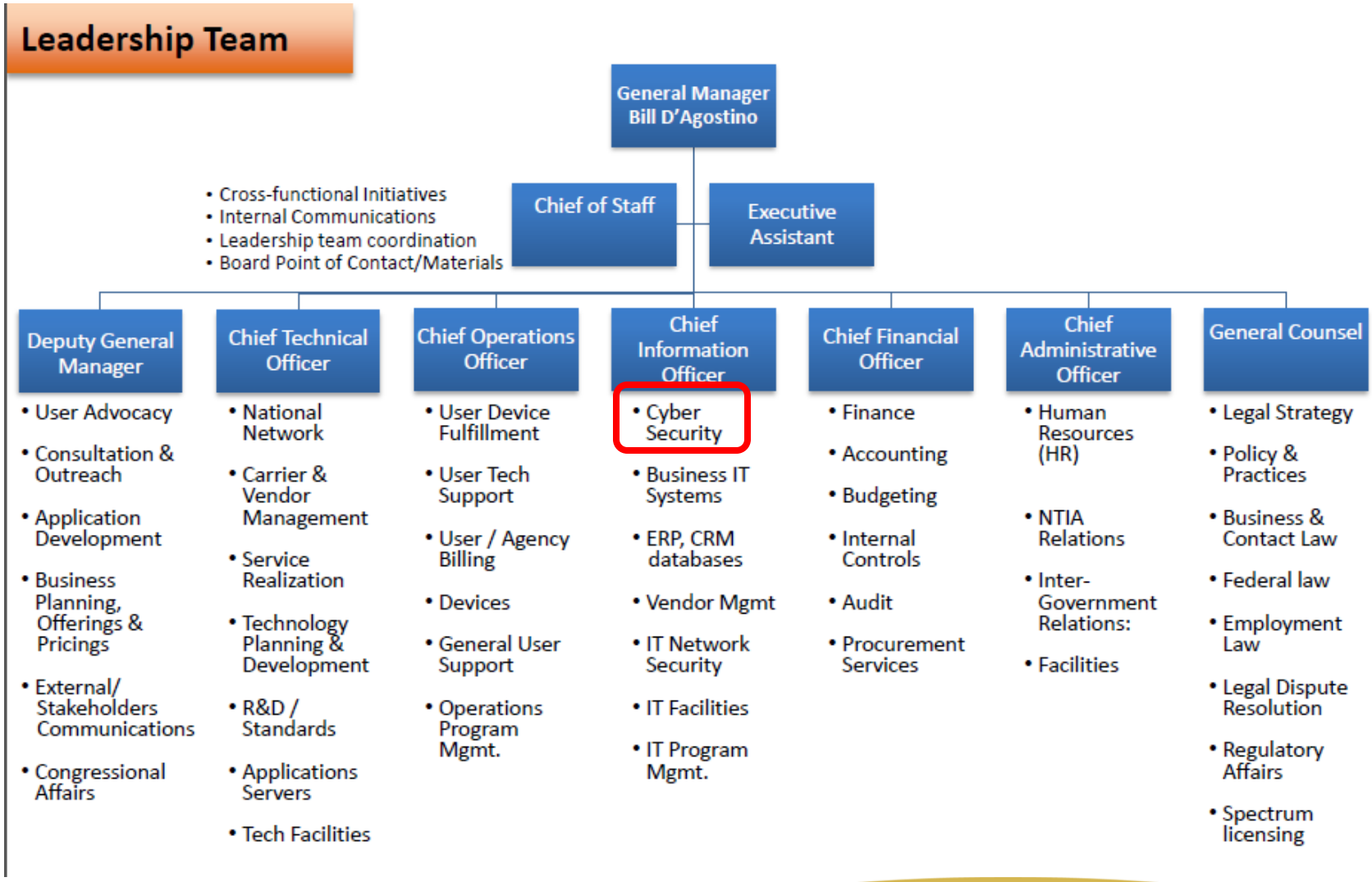
- The NPSBN will face unprecedented Cyber Threats

- The threat is recognized by government agencies, the Spectrum Bill and the FirstNet executive leadership

# Network Security Domains in the NPSBN



# FirstNet Organization Acknowledges Priority

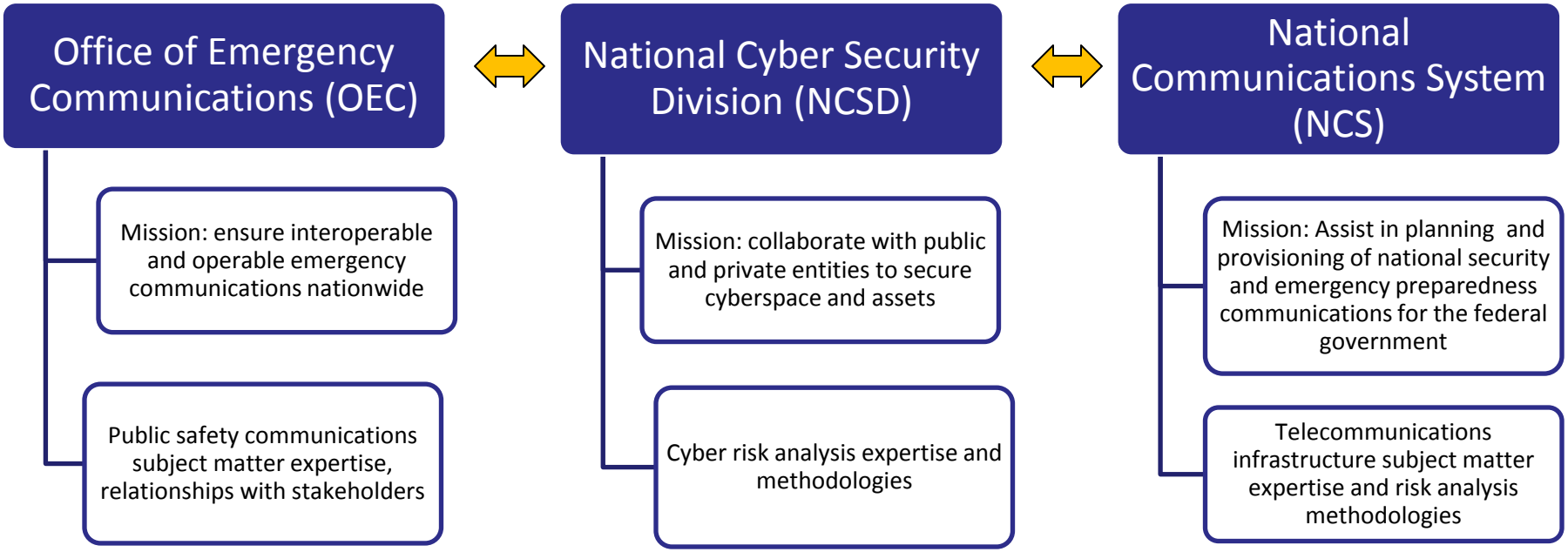


# DHS Cyber Risk Assessment - Background

- Holistic view of new risks brought by the NPSBN
- Identifies cyber risks to enhance the NPSBN from the outset
- DHS has the lead in assessing nationwide cyber risks to civilian agencies and infrastructure
  - DHS Office of Cyber Security and Communications (CS&C)
    - Performs cyber risk assessments for critical infrastructure sectors and federal government agencies
    - Leverages established cyber risk assessment methodologies to identify threats, vulnerabilities, and consequences for NPSBN
  - Input and feedback from public and private sector stakeholders is critical to DHS cyber risk assessments

# Who is Performing the Cyber Risk Assessment?

Collaborative effort between components of the DHS CS&C




- In coordination with other key NPSBN entities, including National Telecommunications and Information Administration (**NTIA**), Public Safety Communications Research (**PSCR**) Program, National Public Safety Telecommunications Council (**NPSTC**).

# Goals of the Cyber Risk Assessment

- Provide results that can be used to better inform policies, priorities, and risk mitigation efforts
  - Inform national-level governance bodies such as the NTIA FirstNet and NIST of risk assessment outcomes.

- Establish a baseline of the current environment noting existing standards, requirements, planning and implementation efforts, and commercially available technologies

- Enable DHS OEC to help stakeholders develop strategies to mitigate and manage cyber risks
  - Guide future policy and service offerings
  - Inform advocacy efforts on behalf of public safety community

# Key NPSBN Cyber Security Initiatives at the FCC

- Emergency Response Interoperability Center – Public Safety Advisory Committee ERIC-PSAC
  - Security and Authentication Workgroup recommendations

- Technical Advisory Board for First Responder Interoperability
  - Topic Area 8: Security

# Cyber Security Methodology Adopted by ERIC PSAC

- Views the NPSBN as an Information System (not just a transport network)
- Bases work on well-established Information Assurance Principles

- NIST Special Publication 800-27 provides the top-down holistic view of the problem
- Identified a list of key objectives for the NPSBN Security Architecture

- Adopted Risk-Based methodology for current and future work

# NPSBN Security Architecture Key Objectives

| | |
|---|---|
| Availability: | Ensure that network services are not disrupted by malicious attacks |
| Privacy: | Ensure protection and integrity of sensitive data and identities |
| Interoperability: | Ensure that security mechanisms do not inhibit interoperability |
| Usability: | Ensure that security-enabled devices and services are easy to use |
| Quality of Service: QoS | Ensure that security mechanisms are not detrimental to achieving QoS required for mission critical applications |
| Cost Effective: | Ensure that the cost of implementing security is consistent with the cost associated with security breach |
| Standards Based: | Ensure robust standards are used for implementing the NPSBN Security Architecture |
| Flexibility: | Ensure that security can be tailored to support role-based security and allow local control and management of security, consistent with the over-arching security policy |

# Risk Based Methodology

| | |
|---|---|
| **Risk** | • Understanding exposure to threats<br>• Assessing likelihood of attack and success<br>• Performing up-front and on-going risk assessments to quantify likelihood and cost of a breach |
| **Threats** | • Understanding source and means of particular types of attack<br>• Performing threat assessments to determine best method(s) of defense<br>• Performing penetration testing to assess threat profiles |
| **Vulnerabilities** | • Weaknesses or flaws in a system that permit successful attacks<br>• Can be policy related as well as technology related<br>• Vulnerability assessment should be performed on an on-going basis |

# NPSBN Security Profile

**Risk**

- Many public safety organizations rely on commercial wireless data services today – that risk profile appropriate for the types of services utilizing these networks
- Increased reliance of the NPSBN by first responders for mission-critical applications will increase that risk profile
- Public safety networks must work when nothing else does, placing a high risk/cost associated with breaches to the security system.

**Threats**

Many types of cyber threats. A representative sample is:

- Denial of Service (DoS) attacks
- Theft of Service (TOS)
- IP address spoofing
- User ID theft
- Intrusion Attacks

Threat environment will evolve over time with more sophisticated attacks in the future

**Vulnerabilities**

- The LTE network will be open to many users
- Many applications will operate over the network
- Access to the Internet may be provided
- Large eco-system of devices with a variety of computing environments will emerge
- The NPSBN will be a frequent target of attack
- Commercial LTE networks will be a frequent target of attack. Because of their connection to a common technology, success of commercial network attack may impact the NPSBN.

# Key Recommendations – ERIC PSAC

- Adopt a risk-based approach to cyber security for the NPSBN
  - Analyze the Risk Profile (balancing impact of breach with cost of protection),
  - Understand the Threat Environment
  - Address/Eliminate Vulnerabilities.
- Accept a Statement of Key Objectives of the NPSBN Security Architecture to serve as guiding principles for implementing cyber security.
- Identify and implement mandatory key LTE standardized security features.
- Support roaming to commercial networks with standardized security technologies.
- Allow access to the Internet, contingent on an acceptable outcome of a full Risk/Threat/Vulnerability analysis.
- Provide support for a diversified set of applications within a varied collection of jurisdictional-specific security policies and implementations by enabling layering of security features on top of a standardized mandatory baseline.

# Key Recommendations of the FCC Interoperability Board

- Requirements
  - Implement Standardized 3GPP LTE security mechanisms over the airlink
    - Control Plane ciphering required
    - Data Plane ciphering optional
  - Implement Standardized 3GPP LTE security in the Core Network
- Recommendations
  - Implement security controls and policy for all entities that access the NPSBN
  - Implement layered security to enable agency-provided end-to-end security
  - Support for a national framework for user identity

HARRIS®
assuredcommunications®

Follow APCO at…

facebook.com/apcointernational

@apcointl

APCO International
Leaders in Public Safety Communications™