APCO International
Leaders in Public Safety Communications™

Securing Public Safety Networks
The APCO Perspective

Jay English, Director
Comm. Center/9-1-1 Services
APCO International

Topics

- Overview
- Environment
- Approach
- Next Steps

Overview

- As Public Safety Answering Point (PSAP) 911 networks transition from TDM-based to IP-based architecture they will face increasing exposure to cyber threats and vulnerabilities that did not exist in the legacy 911 environment.
- Existing work including the NIST Cybersecurity Framework, the ongoing work of CSRIC and the FCC, the recently formed FCC TFOPA and other foundational documents, can assist in cyber risk management strategies for the ecosystem as a whole
- Cyber risk management strategies must be implemented at multiple levels from core services to the PSAP level.

Overview

- Advanced technologies are becoming more integrated into public safety communications networks
- New and emerging cyber risks are an increasing concern
- Many initiatives to mitigate and combat these risks are underway in both the public and private sectors to keep these systems safe and secure

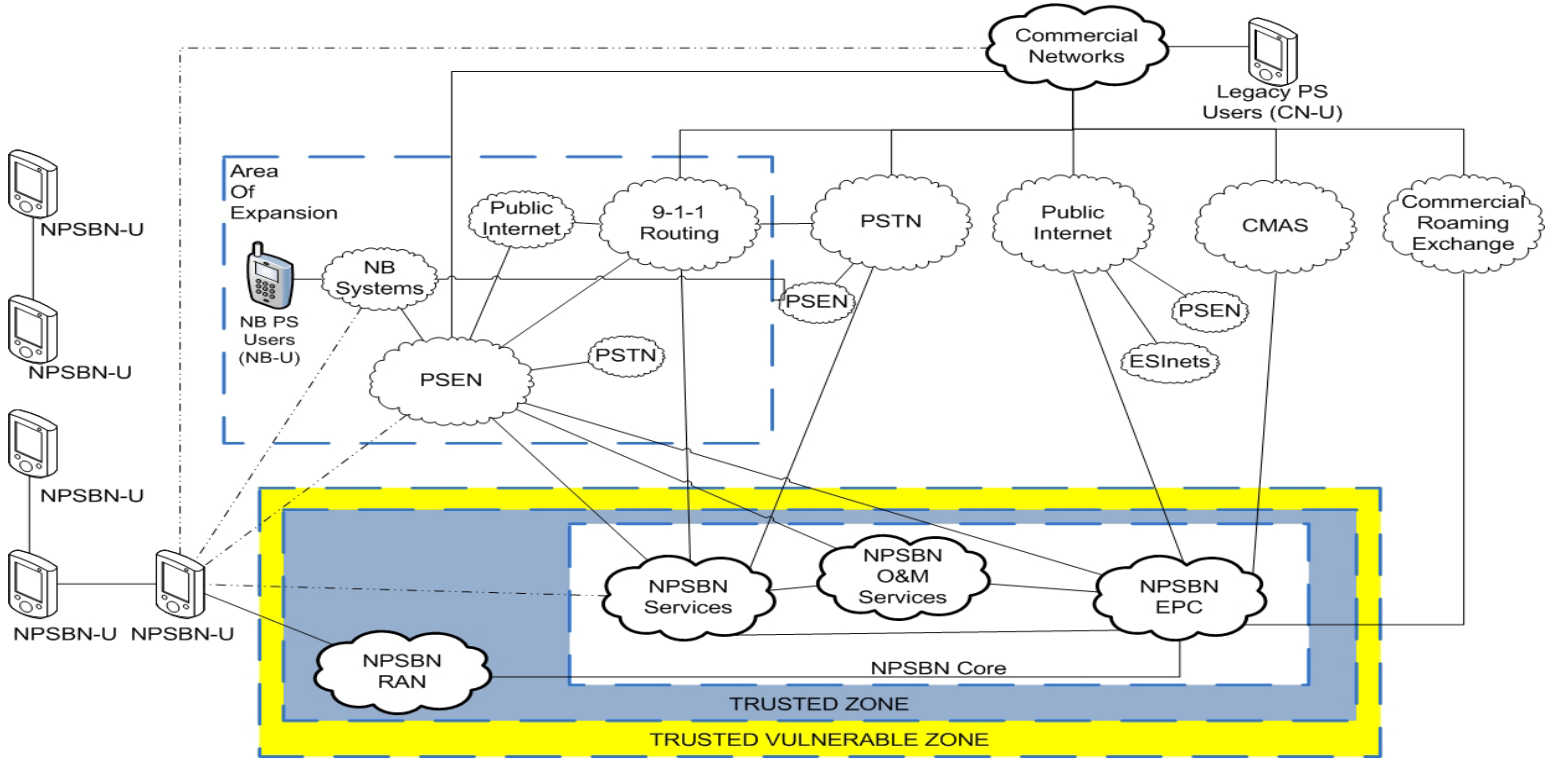
The Threats

- **Destruction:** Physical destruction of information or communications systems rendering them unusable
- **Corruption:** The changing of information such that it is no longer accurate or useful
- **Removal:** The removing of information so that it cannot be accessed, but is not destroyed
- **Disclosure:** Unauthorized release of confidential or sensitive information to the detriment of owner of said data
- **Interruption:** Interfering with communications such that legitimate users cannot send or receive messages

Environment

- Secure communications are a core requirement for PSAPs.
- Requirements to consider may include user credentialing, access control, authentication, auditing, confidentiality, data integrity, physical security, and applications.
- High level network requirements include services, device management and identity management.
- Services may be provided by a central authority and delivered through either centralized or distributed service mechanisms
- May want to consider the concept of a “trusted zone” and a “trusted vulnerable zone”.

Trusted Zones



The Approach

- A realistic self assessment for public safety communications entities and agencies to evaluate their current cybersecurity capabilities and risks;
- A roadmap for the creation and implementation of a successful Cybersecurity strategy that applies to local public safety levels of government, up to and including State level government
- Cyber risk mitigation strategies for interconnectivity with potential federal level resources and capabilities.

The Approach

- Given the scope of Next Generation communications networks and systems as a whole, it is impossible to delve into Cybersecurity considerations for PSAPs without taking into account the existing capabilities of the eco-system of various commercial providers who interact with public safety.
- These include, but are not limited to,
  - 911 Customer Premise Equipment (CPE) providers, Computer Aided Dispatch (CAD) providers, Records Management Systems (RMS) providers, Radio/Dispatch Console providers, Mobile Data providers, Telecommunications Network & Service providers, Public safety database infrastructure providers, and providers of interconnect services at both the voice and data levels.

The Approach

- In addition to discussions that identify the threats already known, and available mitigation strategies, focus should be placed on procedures to Respond, Remediate, Restore and Resolve (“the 4R’s).
- Suggested steps include both notification and recognition of an attack occurring in network elements outside the direct control of PSAPs.

The Approach

- Not only the physical elements of cybersecurity should be addressed. As noted in much of the work already done by NIST and DHS, the human factor is vital when preparing for and defending against cyber threats.

- Personnel security including cyber hygiene, training, and other mitigation steps related directly to the personnel involved with day to day operations and maintenance of any public safety system is key.

Next Steps

- The success of any cybersecurity strategy is rooted in the ability to identify assets, owners of these assets, threats/risks to these assets, and methods to mitigate the threats/risks.
- Forward looking issues must be examined to expand the context of the threat to the public safety communications as a result of the expansion of the public safety ecosystem
- This must include additional information sources and new “players” such as FirstNet, Health care providers, public safety “Apps”, and other entities that reflect the emergence of new technologies.

Cybersecurity is a Risk for Public Safety

The security “DNA” of our networks will define our success