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
- TFOPA Cybersecurity Report
- The Future

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”.

APCO International
Leaders in Public Safety Communications™

Cybersecurity : Optimal Approach for PSAPs

FCC Task Force on Optimal PSAP Architecture
Working Group 1 - Cybersecurity

The defined scope of this work was limited to the identification of cybersecurity issues and documentation of recommended cybersecurity practices for Public Safety Answering Points. However, in the context of this work effort, a local PSAP is much more than a stand-alone entity but rather is the connection point in a complex system of integrated networks that form the critical infrastructure necessary to enable delivery of life saving services. Therefore, as a necessity, there must be reference to other network elements outside of the local PSAP construct.

FCC Task Force on Optimal PSAP Architecture
Working Group 1 - Cybersecurity

- The reduction of any cybersecurity framework to practice is rooted in the ability to identify assets, owners of these assets, threats/risks to these assets, and methods to mitigate the threats/risks.
- Current and NG architectures serve as a starting point to understand the PSAP ecosystem.
- Forward looking issues tused to expand the context of the threat to the PSAP as a result of the expansion of the public safety ecosystem.
- Use cases are used to communicate the types of cybersecurity threats to PSAPs
- Finally, based on the foregoing, the Working Group developed a checklist and roadmap for PSAPs and a set of recommendations.

FCC Task Force on Optimal PSAP Architecture
Working Group 1 - Cybersecurity

- Overarching Information Security Management System (ISMS)
  - Documented Policies, Procedures and Controls in support of the ISMS
  - Compliance
  - Awareness
- Access Control
  - Policy identifies proper approval based on access gates and ratings
  - Physical Security – Limited access and based on need to know
  - Human Resources

FCC Task Force on Optimal PSAP Architecture
Working Group 1 - Cybersecurity

- Security Controls
    - Business Continuity Plan/Disaster Recovery (BCP/DR)
    - Geo-diverse in Active/Active or N+1 configurations
    - Media Handling
    - Incident Management
    - Vulnerability Management
- Internal network security and monitoring
    - Internal network security, Private DNS (internal facing only)
    - External network connections
- Network entry point security

FCC Task Force on Optimal PSAP Architecture
Working Group 1 - Cybersecurity

- NIST Cybersecurity Framework (NCF)
- Identity Credentialing Access Management (ICAM)
- DHS recommendations and resources
- NICE Workforce Framework
- CSRIC Best Practices Related to Public Safety

FCC Task Force on Optimal PSAP Architecture
Working Group 1 - Cybersecurity

- U.S. Department of Commerce
  - NIST: Cybersecurity Framework
  - NIST: Cyber Physical Systems- Public Work Group Report
    - Relationship To PSAPs: Identify, Protect, Detect, Respond, Recover
  - NICE Workforce Framework
    - Relationship of occupational specialties to PSAPs
    - Define any new/missing occupational specialties
    - Consider Cyber Professional Best Practices for PSAP workforce

FCC Task Force on Optimal PSAP Architecture
Working Group 1 - Cybersecurity

- Department of Homeland Security
  - Critical Infrastructure Cyber Community Voluntary Program (C3VP)
  - Critical Infrastructure Cyber Information Sharing and Collaboration Program (CISCP)
  - Cyber Reports & Recommendations
  - Cybersecurity Products & Solutions:
  - National Cybersecurity and Communications Integration Center (NCCIC)
    - NCCIC/National Coordinating Center for Communications (NCC)
    - NCCIC/United States Computer Emergency Readiness Team (US-CERT)

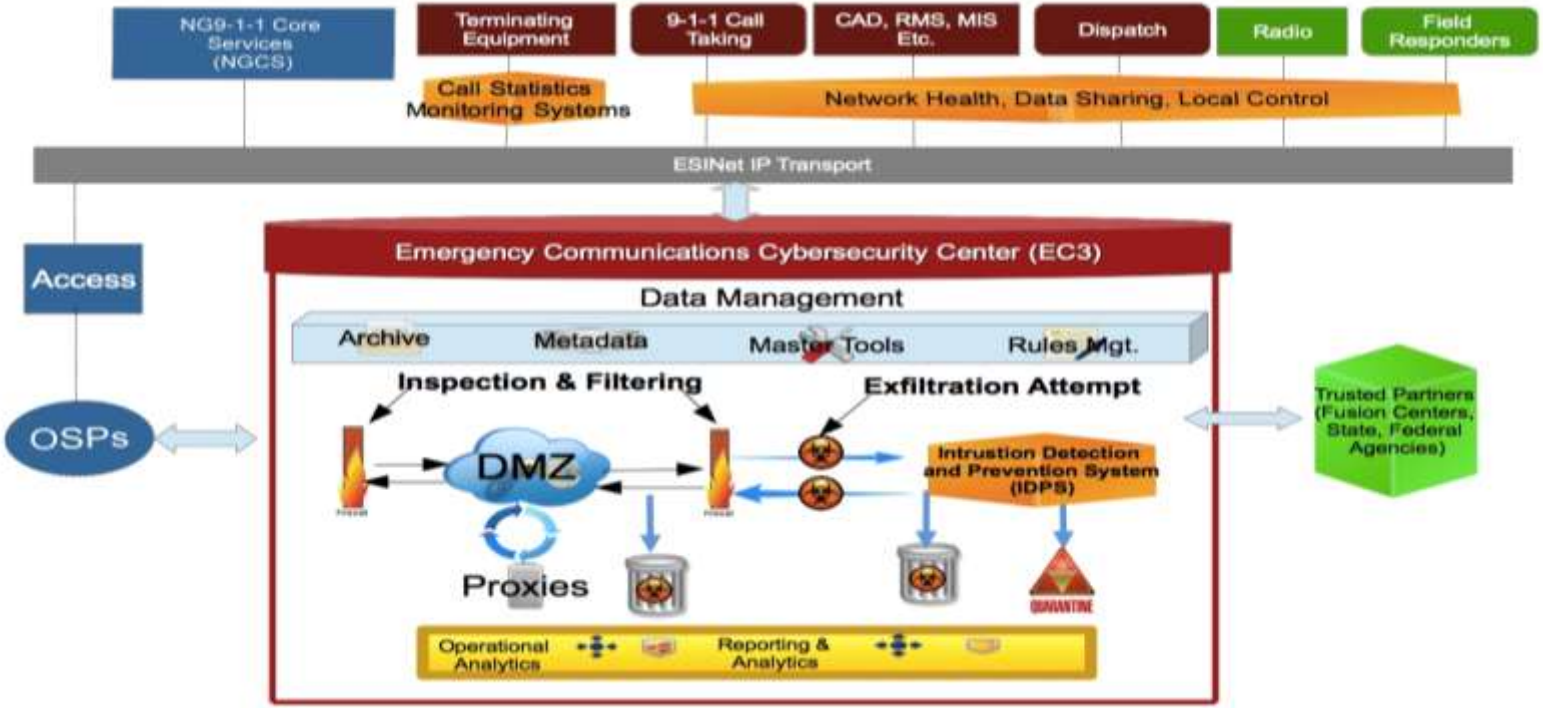
Cybersecurity For The Future

- The threat is real and increasing
  - TDoS and DDoS attacks have occurred, and continue to occur in a legacy environment
  - Both criminal and Nation State actors are involved
- This threat will increase exponentially as we transition to IP based architectures
- We must think “outside the box” and consider unifying, information sharing based, architectures and options.

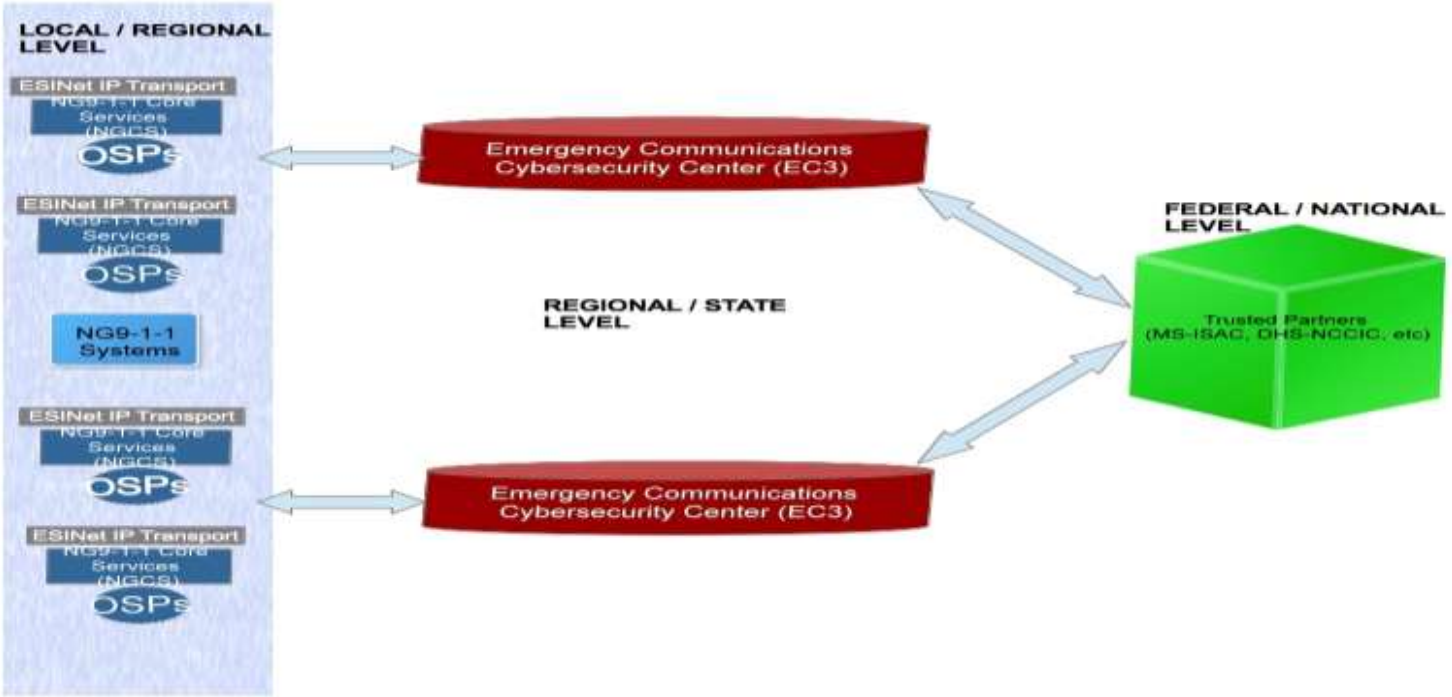
Cybersecurity Architecture Options For The Future

- The Emergency Communications Cybersecurity Center (EC3)
  - Description of Intrusion Detection and Prevention Systems
  - Proposed Approach for IDPS in the NG9-1-1 Environment
- The EC3 Concept Explained
- Cost Considerations

Emergency Communications Cybersecurity Center



Distributed Integration of EC3 Deployments



Cybersecurity Plan For The Future

- PSAPs: Funding The Cybersecurity Plan
- Discussion of basis for cost estimates
- Funding Opportunities
- The importance of information sharing and partnerships

Appendix 1- PSAP: Cybersecurity Use Cases

- Specific Use Cases Addressing:
  - TDoS
  - DDoS
  - SWATTING
  - Single PSAP Compromised, Need exists to protect Interconnected PSAPs

Appendix 2: Cybersecurity Best Practices for PSAPs

- PSAP Cybersecurity Checklists
- Roadmap to secure PSAPs
- Cybersecurity Life Cycle Roadmap Example
- Starting Activities for Basic Security Hygiene

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