

Cyber Security and Next Gen Systems



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

Topics to Cover

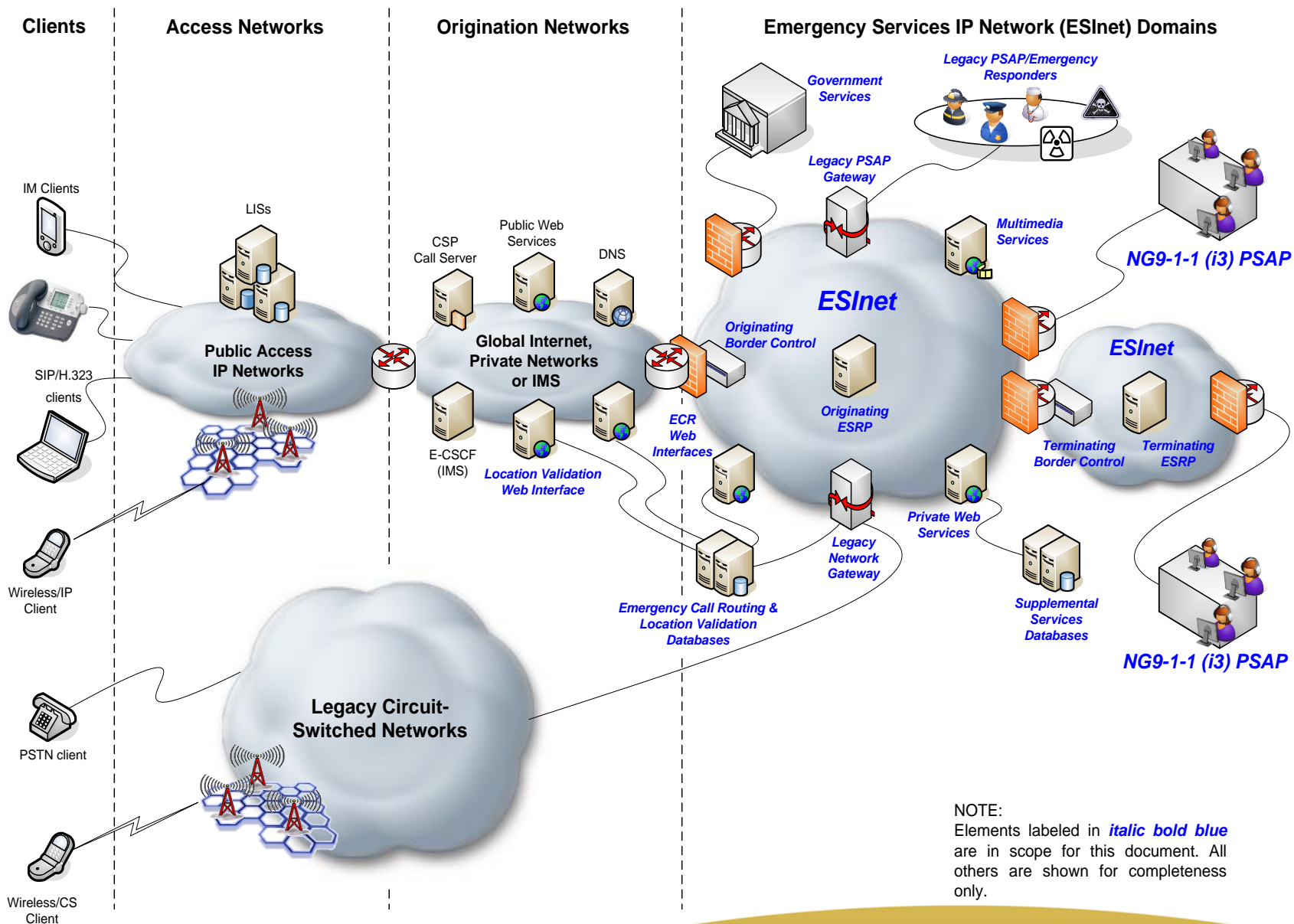
- **NG9-1-1 – Emerging technology and emerging threats**
- **Basic types of threats**
- **FirstNet and Security**
- **Planning and Preparation**

“NG9-1-1?”

- Legacy 9-1-1 systems are relatively secure, and while threats exist they are somewhat limited
 - TDoS
 - Carrier outages
 - Capacity issues
- While secure, the system is extremely dated and limited.
 - Location limitations
 - Media capabilities
 - CAMA trunks / Circuit switched technology

“NG9-1-1”

- Next Generation systems will be a “network of networks” providing connectivity between PSAPs on a network within a specified geographic area to other networks both regionally and nationally
- With advancement of technology comes an increased threat of infiltration and exploitation of the system
- Reliant on data rather than traditional voice
- NG9-1-1 systems and ESINets will be vulnerable to the same threats as existing IP networks and systems



NOTE:
Elements labeled in *italic bold blue* are in scope for this document. All others are shown for completeness only.

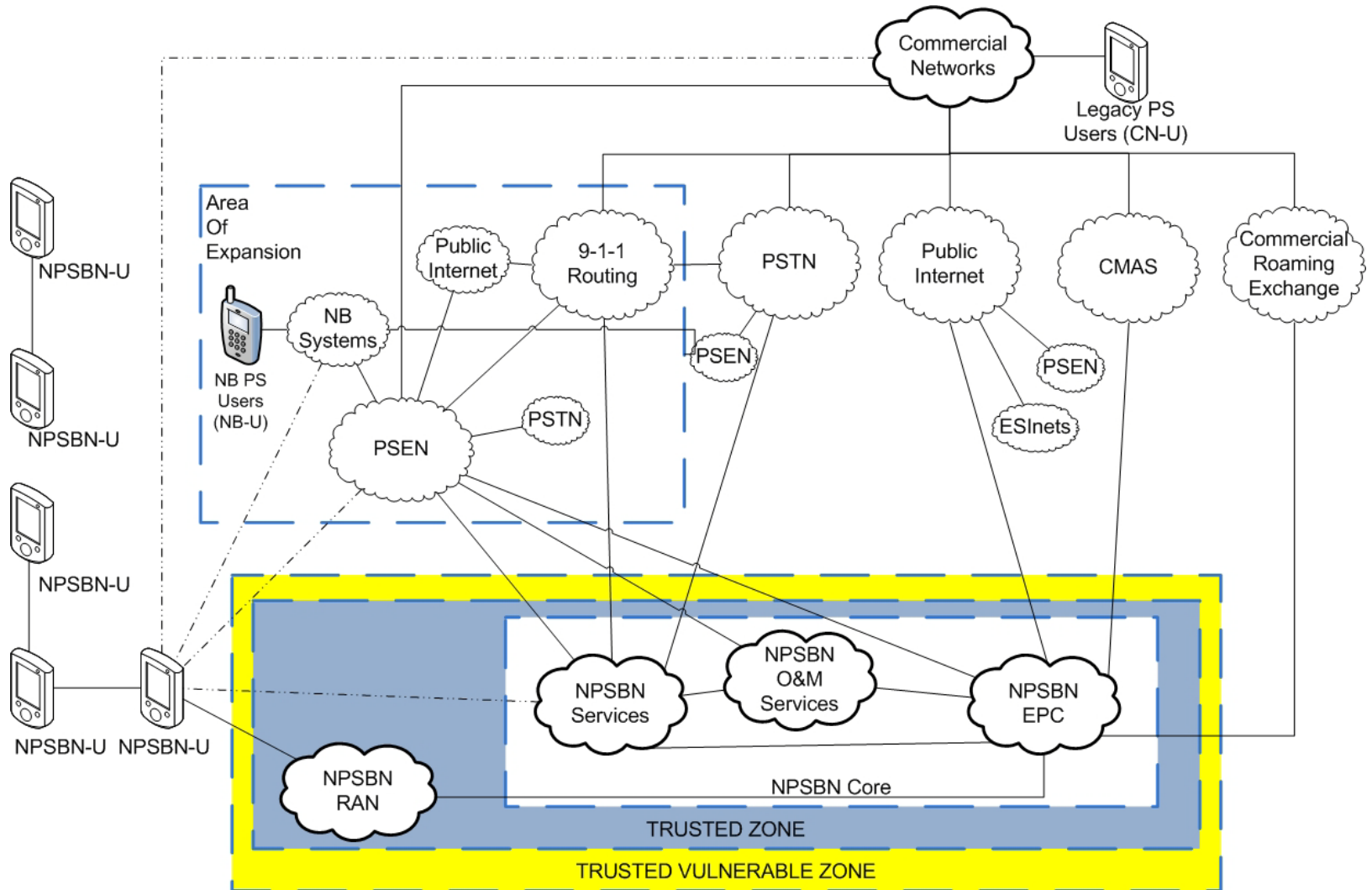
Types of Threats

- **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

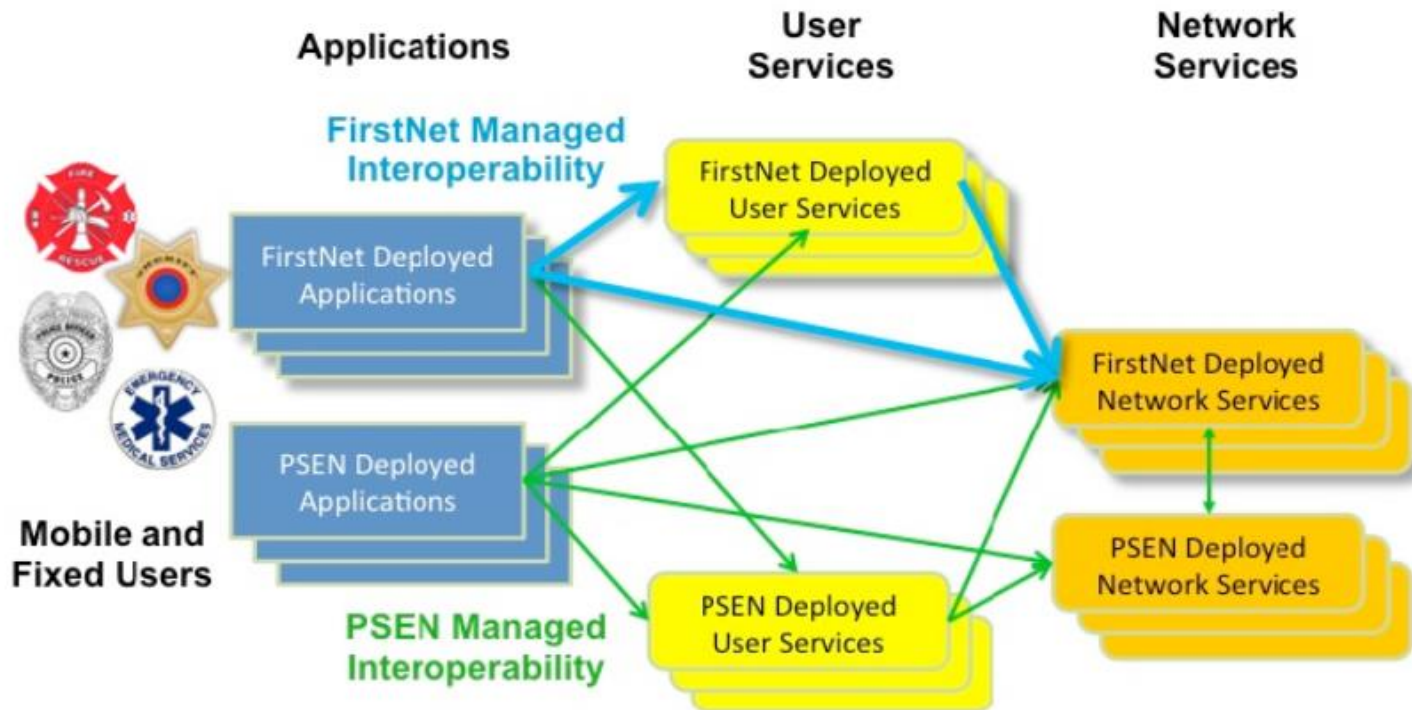
Cyber Security and FirstNet

- Secure communications are a core requirement for FirstNet
- Requirements 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
- Included in the security specifications under consideration is the concept of a “trusted zone” and a “trusted vulnerable zone”

Trusted Zones



FirstNet Apps



Examples

- | | | |
|---|--|---|
| <ul style="list-style-type: none"> • Advanced multimedia telephone • Video • PTT Apps • Fire situational awareness, etc. • Computer-Aided Dispatch | <ul style="list-style-type: none"> • Cellular Telephony • Video • Direct-mode PTT (not for Launch) • Messaging, etc. | <ul style="list-style-type: none"> • Location • Service Discovery • DNS • Identity • Dynamic QoS, etc. |
|---|--|---|

Planning and Preparation

- Have a pre-plan. The TDoS attacks resulted in activation of a task force to provide best practices and much needed cooperation amongst multiple parties. Those best practices can be found here: <http://psc.apcointl.org/2013/03/28/telephony-denial-of-services-tdos-to-public-safety-communications-phone-service/>
- Learn about NG9-1-1. There are a number of resources available to provide education on NG9-1-1 and emerging technologies. Here are a couple of places to start: <http://www.apcointl.org/resources/next-generation-communications-systems.html>, <http://www.ng911institute.org>.

Planning and Preparation

- Look into available security options for the networks all the way to the PSAP equipment level. Consider what your records systems will integrate with, your CAD and mobile requirements, recording and retention requirements, and integration of any outside network into your “closed” PSAP or jurisdictional systems.
- Research FirstNet and emerging Apps: FirstNet is exciting technology and will bring some tremendous capabilities to the public safety community. APCO encourages all members of the public safety community to begin researching, and understanding, the networks and systems that will make up FirstNet here:

<http://www.ntia.doc.gov/category/firstnet>.

Planning and Preparation

- Once you have a fundamental understanding of the concepts here, look into the Security and Priority sections of the FirstNet Statement of Requirements, found here:
http://www.npstc.org/download.jsp?tableId=37&column=217&id=2609&file=BBWG_SoR_Launch_12112012.pdf.
- This research into security requirements provides you with a “toolbox” of information and questions as well as some design considerations for your own systems.

Planning and Preparation

- In addition to the actual FirstNet system, applications will play a key role in public safety. Today, apps are fun and convenient ways to send messages, retrieve information about a selected topic, or even find the closest place to eat when you're traveling. Tomorrow, they will provide life saving services and links to public safety in near real-time. Understanding the make up of emerging apps is critical to understanding how our networks of tomorrow will work. APCO has established a web site specifically designed to provide public safety professionals with a "one stop source" of information on public safety related apps. The site can be found here: <http://appcomm.org>.

Evolution not Revolution

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

