APCO International

Leaders in Public Safety Communications™

Cybersecurity & Mobile Apps

Jay English

Director, Comm Center & 9-1-1 Services

Jeff Cohen

Chief Counsel, Law & Policy

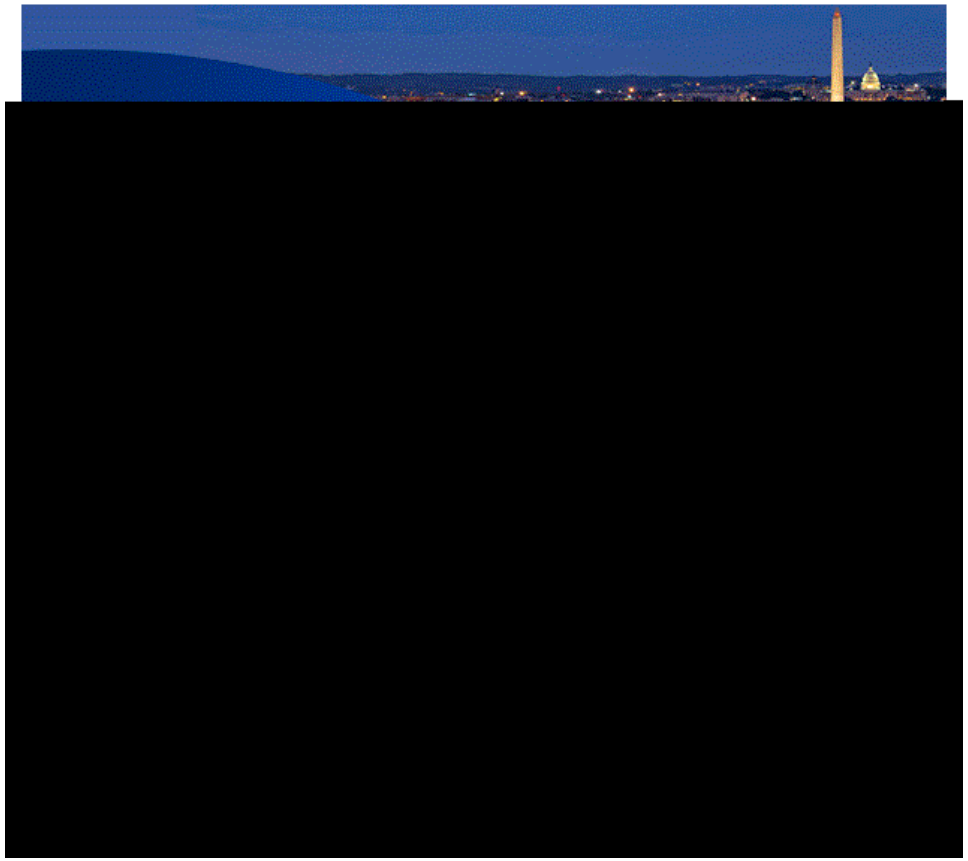
APCO International

November 5, 2014

APCO & Cybersecurity

- 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

New Cybersecurity “Trending” Button



Cybersecurity Resource

- Debuted during National Cyber Security Awareness Month (October)
- Page contains relevant information from industry, the federal government, and APCO

APCO

ANNOUNCEMENTS

- National Cyber Security Awareness Month 2014: Guidance for Public Safety Communications Professionals October 2014
  October 2014
- National Institute of Standards and Technology Seeks Input Following APCO Workshop on App Security Requirements: Opportunity for APCO Members to Contribute Professional Expertise
  August 8, 2014
- Cybersecurity & the PSAP: Protecting Against Malicious Cyber Activity
  March 2014
- Telephony Denial of Services (TDOS) to Public Safety Communications Phone Service: Recommended Best Practices Checklist
  March 28, 2013
- UPDATED BULLETIN - TDoS Attacks
  March 15, 2013

PUBLIC FILINGS

- FCC's Public Safety and Homeland Security Bureau Requests Comment on Implementation of CSRIC III Cybersecurity Best Practices
  - APCO Comments

  September 26, 2014

APCO's CC9S Team Releases Cyber Security White Paper

National Cyber Security Awareness Month 2014: Guidance for Public Safety Communications Professionals

Introduction

Public safety communications systems are becoming more integrated with advanced technologies than ever before. These developments bring both the promise of new capabilities, and the inherent issues of cyber security. The phased implementation of Next Generation 9-1-1

- Document identifies potential types of attacks to which public safety agencies and employees may be susceptible
- Covers prevention, mitigation, and reporting strategies

Emerging Technologies – Emerging Threats

- Basic types of threats
- FirstNet and Security
- Planning and Preparation
- Apps

APCO International
Leaders in Public Safety Communications™

Legacy vs Next Gen

- 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

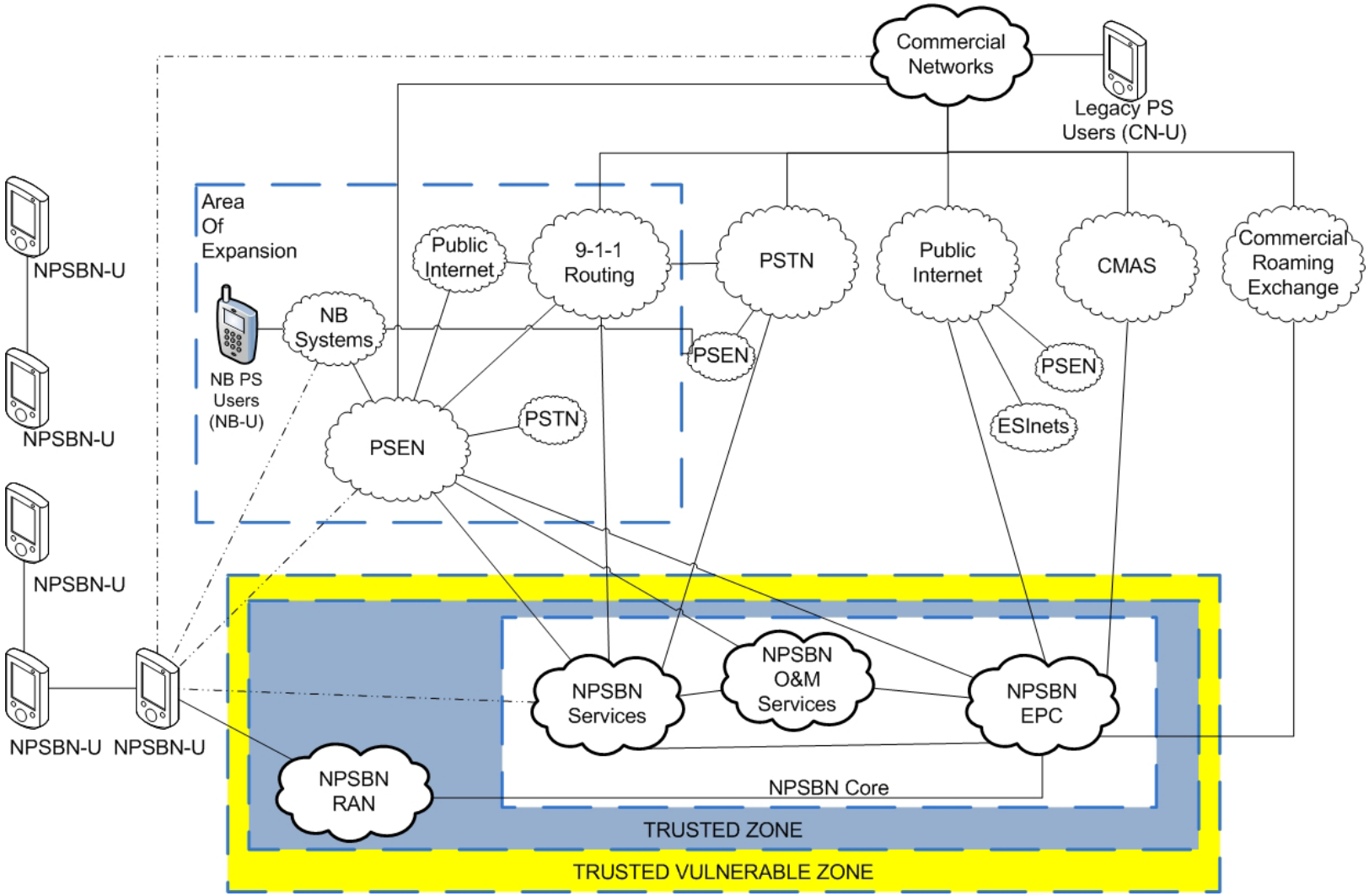
Types of Threats

- **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

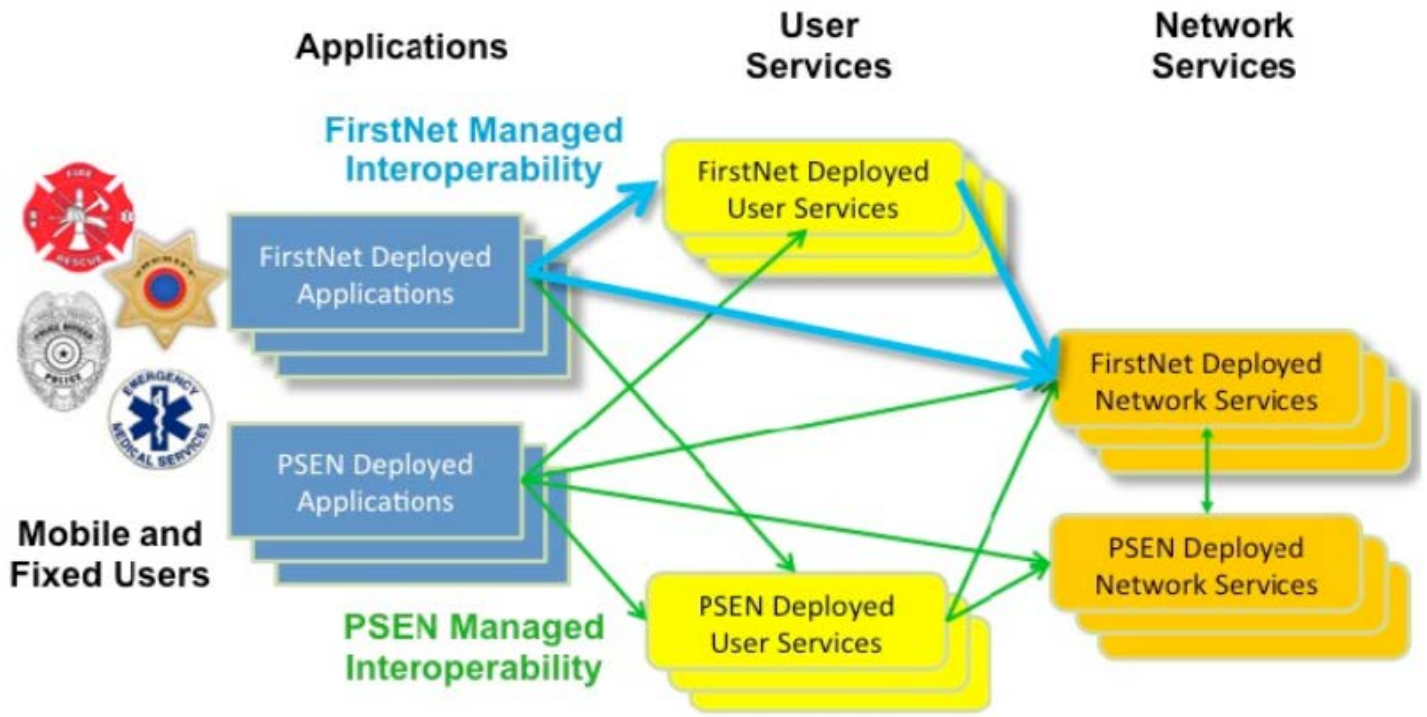
- Secure communications are a core requirement for FirstNet
- Requirements include user credentialing, access control, authentication, auditing, confidentiality, data integrity, physical security, and applications
- High level network requirements include services, device management and identity management
- 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



APCO International
Leaders in Public Safety Communications™

FirstNet Apps



Examples			
	• Advanced multimedia telephone	• Cellular Telephony	• Location
	• Video	• Video	• Service Discovery
	• PTT Apps	• Direct-mode PTT (not for Launch)	• DNS
	• Fire situational awareness, etc.	• Messaging, etc.	• Identity
	• Computer-Aided Dispatch		• Dynamic QoS, etc.

APCO International
Leaders in Public Safety Communications™

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.**

APCO International
Leaders in Public Safety Communications™

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.
- To many consumers, Apps are convenient ways to send and retrieve information about a selected topic, or even find the closest place to eat when you're traveling.
- They can also 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.

Planning and Preparation

- Also critical is the need to understand the difference between secure and non-secure apps, and open standards based apps vs. proprietary single solutions.

- 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**.

APCO's Key Attributes

- APCO created a list of Key Attributes of Effective Apps for Public Safety and Emergency Response to guide the selection of apps on AppComm. They include:
  - **Operability** (efficient use of data, minimal battery strain)
  - **Security** (free of malicious code, supports identity management)
  - **Privacy / Confidentiality** (proper treatment of private data)
  - **Communication with 9-1-1, sending data to PSAPs and Comm Centers, and interfacing with PSAPS** (NOTE: APCO has filed a PIN with ANSI to develop a standard for apps that interface with communications centers and public safety responders)
- APCO is seeking partnerships with industry leaders to assist with testing apps to ensure maximum effectiveness and reliability
- Contact us at AppComm@APCOIntl.org

App Security Workshop

NIST/APCO Workshop – App Security Requirements for Public Safety

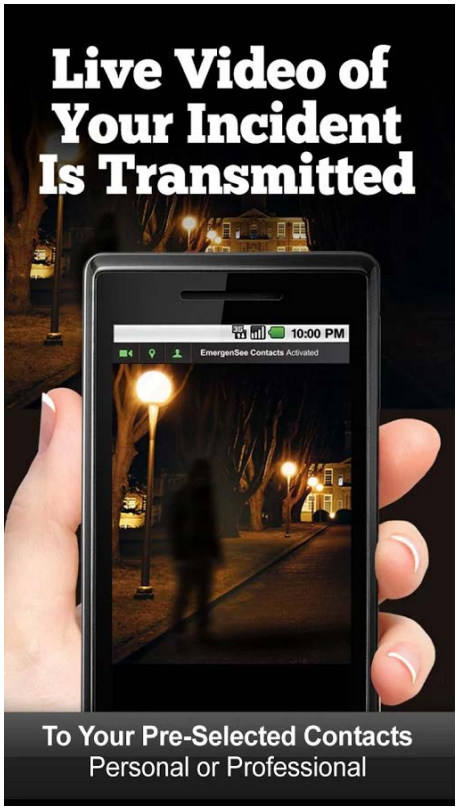
- Co-located with APCO's Emerging Technology Forum in Orlando
- Input from public safety practitioners, app developers, and industry experts
- Output will be a NIST report

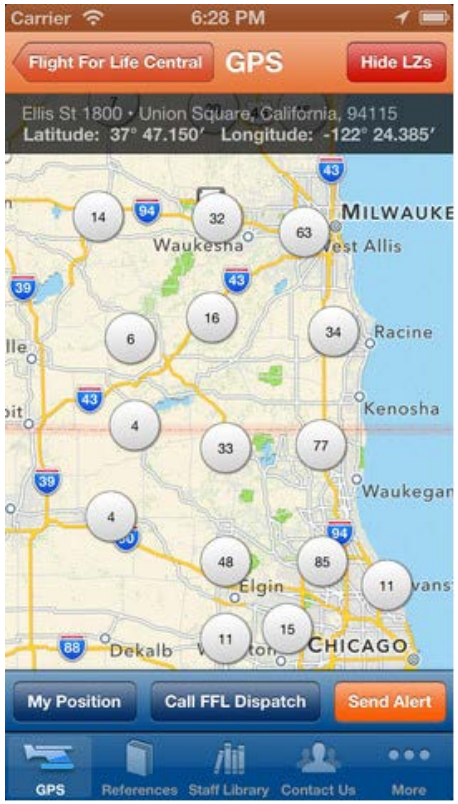
APCO International
Leaders in Public Safety Communications™

Operability

- *Efficient use of data; minimal strain on battery life*

Some features that will be especially useful for public safety require particular attention for data and battery efficiency.





APCO International
Leaders in Public Safety Communications™

Security Topics

- Battery life
  - Power drain can quickly become a security issue
  - Apps should report battery impact
  - Create power management profiles specific to responder types
  - Explore remote power management tools

Security Topics

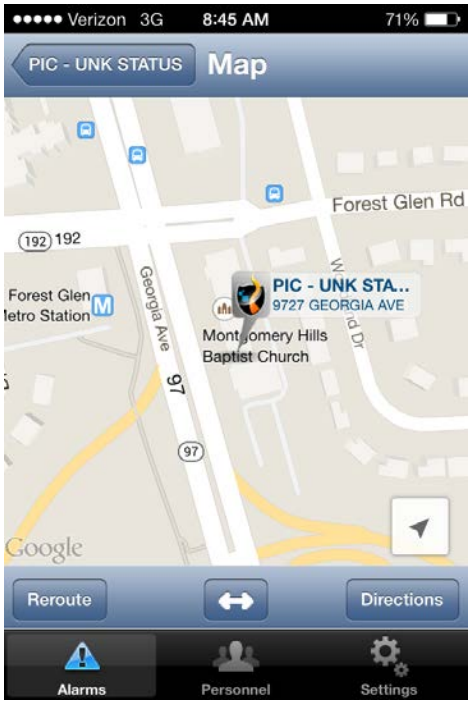
- Unintentional Denial of Service (UDoS)
  - Potential of multitudes of first responders saturating local cells with data such as voice, location and of most concern, video
  - Explore how LTE QoS levels and remote management can mitigate

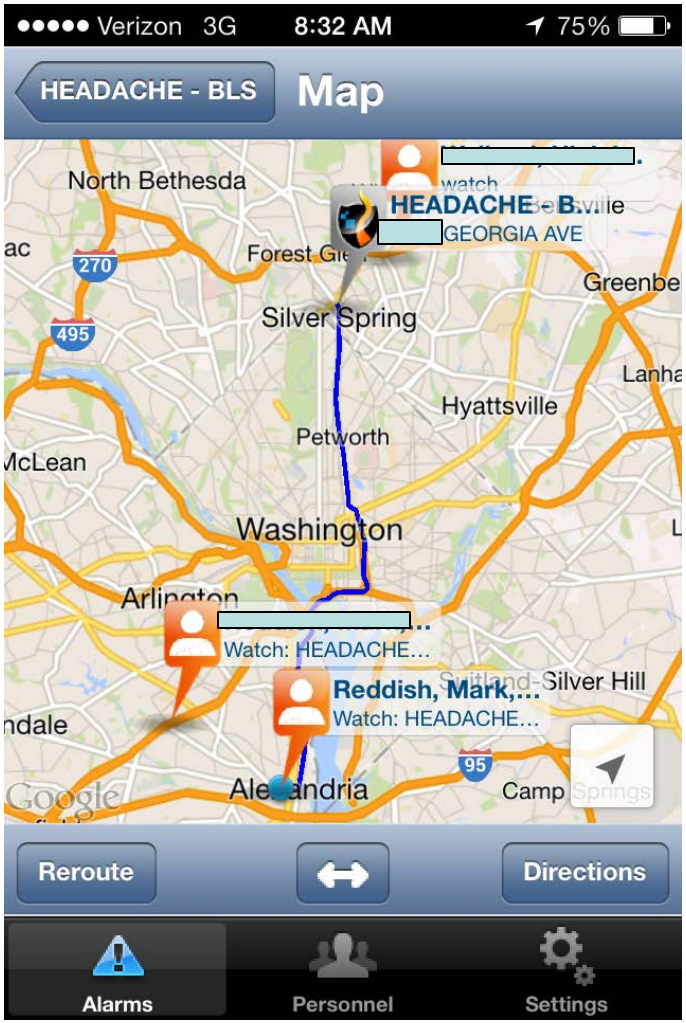
Security Topics

- Mobile App Vetting
  - Free from malicious code and known vulnerabilities
  - Establish a test process and trusted registry
- Data Protection
  - Sensitive info must be protected against unauthorized disclosure and modification
  - Need to identify specific data types and protection requirements

Location Information

- *Adequate safeguards are in place to protect privacy, confidentiality*





APCO International
Leaders in Public Safety Communications™

Security Topics

- Location Information
  - Sub-category of data protection
  - Evaluate standards for exchanging location info and central management
- Identity Management
  - Identified a need to establish a hierarchy of authentication to account for the situation at hand

Workshop Use Case Example

- *During a medical emergency response, a paramedic uses a mobile application to collect a patient's information (name, age, gender, age, etc.) as well as to monitor the patient's vital signs (heart rate, blood pressure, temperature, etc.). In addition, the mobile application forwards the patient information to the hospital the patient will be taken to.*
  - *How much of this is "sensitive" information?*
  - *Do legal/regulatory requirements cover it?*
  - *How is sensitive data identified and labeled?*

Next Steps

- Publication of NIST Report
- Key Attributes Update
  - Ex – App location features must be configurable either by the users or admins, and/or by location/mission-based profiles
- Additional Research
  - Ex – Evaluate the effectiveness of existing metrics for battery usage and establish metrics relevant to public safety operations