



# Homeland Security

## **Office of Emergency Communications (OEC) Mobile Applications for Public Safety (MAPS)**

PSCR Public Safety Broadband Stakeholder Conference  
June 4<sup>th</sup>, 2014

Alex Kreilein  
Technology Policy Strategist  
Office of Emergency Communications

# Lives and property depend on a stable, safe, and resilient cyberspace for first responders.

- Broadband technologies may introduce new cyber threats that the public safety community has not had to address in the land mobile radio (LMR) environment
  - Public safety data is a high-value target for hackers, criminals, and terrorists
  - Cyber threats are increasing and becoming more sophisticated
  - Mobile cyber threats unique to public safety are not well understood
- Given the type of data that public safety collects and produces, consequences could be severe if proper security measures are not implemented
  - Medical information and patient history
  - Critical infrastructure information
  - Sensitive investigative, dispatch or operational information
  - Personally Identifiable Information (PII) (e.g., Social Security Numbers, birthdates)
- Trust in broadband communication and mobile applications must be established for them to support public safety's critical missions and sensitive information



# To establish trust in the technologies, cyber risks must be qualified, quantified, and mitigated.

- “Cyber risks” are anything that would negatively impact the security and resiliency of the cyber infrastructure
  - Cyber security refers to the confidentiality, integrity, and availability of the data
  - Resiliency refers to the ability of the infrastructure to maintain continuous operability
- Key risk terms:
  - **Threat:** natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property
  - **Vulnerability:** physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard
  - **Likelihood:** chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies, or probabilities
  - **Consequence:** effect of an event, incident, or occurrence

**Risk = the *likelihood* of a threat exploiting a vulnerability and the potential *consequence* or impact of that event**

Source: DHS Risk Lexicon. <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>



Homeland  
Security

Office of Emergency Communications

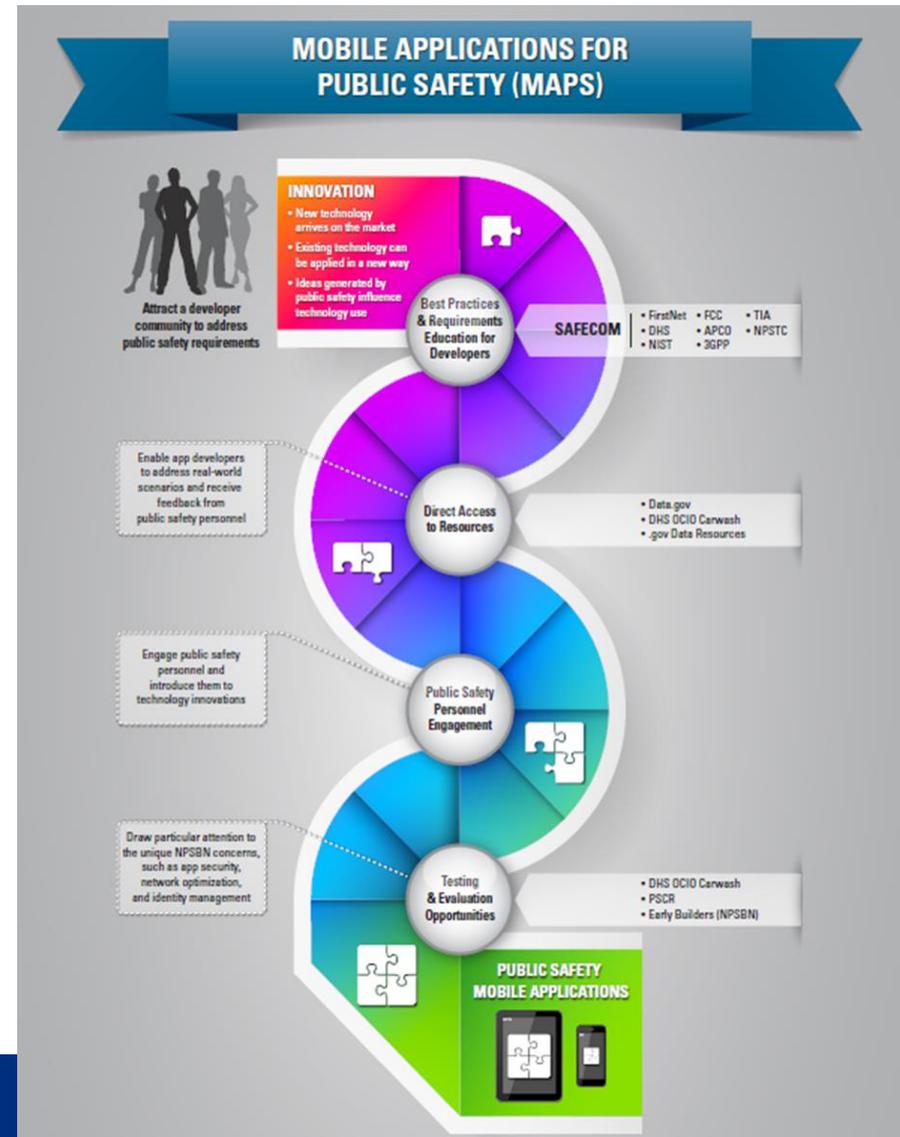
# Our recent, risk-based analysis showed mobile apps as producing high-likelihood and high-consequence risks.

Scenario Short Name	Scenario Explanation	Network Section	Threat Type	Likelihood	Consequence	Impact
Malware (RAN)	A malicious threat actor uses malware to exploit the network infrastructure, systems, or applications on the RAN	RAN	Deliberate	High	High	<ul style="list-style-type: none"> <li>• Malware embedded in hardware, software, applications</li> <li>• Viruses, worms and hijack attempts damage infrastructure</li> <li>• Malicious applications (e.g., keyloggers) steal data</li> <li>• Spear-phishing attack gets data from PS official</li> </ul>
Database Attack or Exploitation	A malicious threat actor exploits database services in the Core	Core	Deliberate	Medium	High	<ul style="list-style-type: none"> <li>• Man-in-the-middle attack allows hacker to gain entry into sensitive data</li> <li>• Open-source database hacking tools used to find vulnerabilities</li> <li>• SQL injections</li> <li>• By exploiting vulnerabilities in connected systems or databases, a hacker might get into one database or system and obtain access to others</li> </ul>



# Mobile Applications for Public Safety (MAPS) provides policy oversight for the public safety mobile ecosystem.

- Collaborates with industry, public safety, academia and government
- Promotes the security, functionality and performance requirements of public safety
- Advocates for public safety mission needs in the mobile environment
- Coordinates the lifecycle of public safety mobile apps development
- Enables and streamlines the development, discovery and distribution of mobile applications for first responders



# MAPS is engaged in activities designed to bolster the ecosystem in cybersecurity and other attributes.

Activity	Impact
<b>Developer Community Outreach</b>	<i>Developer and vendor relationships are key to establishing a lasting public safety apps ecosystem and capitalizing on the efficiencies of the existing market.</i>
<b>Policy Shaping</b>	<i>MAPS can translate commercial app ecosystem elements (e.g., app store implementations, testing and evaluation, security techniques) to inform apps requirements processes for first responders.</i>
<b>Educational Materials for Public Safety</b>	<i>Understanding the benefits and challenges associated with mobile applications will assist public safety in incorporating them appropriately into their operations.</i>
<b>Educational Materials for Developers</b>	<i>Understanding and interacting with the public safety community can improve developers' impact, and introduce public safety's unique operational environment challenges.</i>
<b>Tools and Testing Identification</b>	<i>Publicizing tools and testing opportunities keeps MAPS participants aware of the latest opportunities to refine app attributes.</i>
<b>Government Community Outreach</b>	<i>Having an public safety and/or FirstNet-focused apps process will assist end users in locating and recognizing trusted apps to support their missions.</i>



## The right person having the right access at the right time to sensitive information is essential.

- **Vulnerability:** Sensitive information exchange is regularly taking place
- **Mitigation Strategies:**
  - Common industry data security practices
  - Established software and data use guidelines
  - Trusted applications marketplace
  - Application programming interfaces (API)
  - Software development kit (SDK)
  - Risk/threat-based approach to protection and encryption
  - Balanced security decisions
  - Standards
  - Network mitigation techniques
  - Secure coding practices
  - Developer and user education
  - Policy establishment and enforcement



# Collecting, aggregating, and presenting information that is valuable and easily accessible is imperative.

- **Vulnerability:** Risks are being identified, communicated, and mitigated in highly stressful situations and conditions
- **Mitigation Strategies:**
  - Operational effectiveness focus
  - Tailored experience
  - Consistent user experience
  - Defined quality user experience
  - Data availability
  - Data validation
  - Consistent data taxonomies and use of metadata
  - Standards
  - Developer and user education
  - Policy establishment and enforcement



# Available, responsive, and resilient communication is necessary for effective response.

- **Vulnerability:** Disruptions to communication for a first responder can mean the difference between life and death
- **Mitigation Strategies:**
  - Tailored experience
  - Consistent user experience
  - Quality user experience
  - Network management mechanisms
  - Priority mechanisms
  - Data volume and speed expectations
  - Features that simplify data analytics, maintenance, and distribution
  - Standards
  - Developer and user education
  - Policy establishment and enforcement



# Case Study: Denial of Service (DoS)

- Denial of Service Description: An attack wherein the victim (i.e. legitimate user) is prevented from accessing information or services
  - Flooding is common (see SYN Flood, Reflection Attack, Smurfing, etc)
- Traditionally, RF DoS targeted lower layers (Typically Layer 3 & Layer 4)
  - Layer 7 is also at risk – perhaps even more devastating
- Mobile Applications are vulnerable to resource depletion exploits
  - Memory Access/Buffer Overflow
  - CPU, Disk Space, Battery Life
  - Bandwidth
- Attack Surface: First Responder Applications & Devices
  - Persons or groups can be targeted
  - Device resource depletion or root/hardware control
- Attack Surface: Network or System
  - Network elements can be targeted
  - Overwhelm the RF link, IP network, or computational elements



# MAPS also has a “*First Responder Mobile Application Development Best Practices Guide*”

- The MAPS best practices guide provides assistance to developers in understanding the public safety market.
- The Guide was developed in conjunction with mobile application developers, public safety personnel, and commercially-available best practices.



- Educates developers on the operational environments of first responders
- Introduces developers to the challenges faced by personnel in each of the public safety disciplines
- Promotes the security, functionality and performance requirements of public safety
- Provides recommendations for enhancing apps specifically for public safety, including resources for further research



# Summary

---

- There are many challenges associated with the development, testing, distribution, deployment and maintenance of mobile applications
- DHS OEC MAPS is advocating for the first responder within the mobile applications ecosystem, and collaborating with industry, academia, and government to address the most pressing issues
- Enabling cybersecurity within the context of the anticipated performance and function anticipated by first responders will be a key to long-term success





# Homeland Security

**Contact Information**  
**DHS\_MAPS@hq.dhs.gov**



**Homeland Security**

Office of Emergency Communications