Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date	May 11, 2020
Original Release Date	December 3, 2018

Superseding Document

Status	Final
Series/Number	NIST Interagency or Internal Report (NISTIR) 8196
Title	Security Analysis of First Responder Mobile and Wearable Devices
Publication Date	May 2020
DOI	https://doi.org/10.6028/NIST.IR.8196
CSRC URL	https://csrc.nist.gov/publications/detail/nistir/8196/final
Additional Information	Security Research Portfolio (Public Safety Communications Research Division) https://www.nist.gov/ctl/pscr/research-portfolios/security

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NISTIR 8196

Security Analysis of First Responder Mobile and Wearable Devices

Joshua M. Franklin
Gema Howell
Scott Ledgerwood
Jaydee L. Griffith

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8196-draft

National Institute of Standards and Technology
U.S. Department of Commerce

Draft NISTIR 8196

Security Analysis of First Responder Mobile and Wearable Devices

Joshua M. Franklin
Gema Howell
Applied Cybersecurity Division
Information Technology Laboratory

Scott Ledgerwood
Public Safety Communications Research Division
Communications Technology Laboratory

Jaydee L. Griffith
Institute for Telecommunication Sciences
National Telecommunications and Information Administration

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8196-draft

December 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency Report 8196
75 pages (December 2018)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8196-draft

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

[12/18/2018: Comment period extended.]

Public comment period: *December 3, 2018* through *February 6, 2019*

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: nistir-8196-comments@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

Public safety practitioners utilizing the forthcoming Nationwide Public Safety Broadband Network (NPSBN) will have smartphones, tablets, and wearables at their disposal. Although these devices should enable first responders to complete their missions, any influx of new technologies will introduce new security vulnerabilities. This document analyzes the needs of public safety mobile devices and wearables from a cybersecurity perspective, specifically for the fire service, emergency medical service (EMS), and law enforcement. To accomplish this goal, cybersecurity use cases were analyzed, previously known attacks against related systems were reviewed, and a threat model was created. The overarching goal of this work is to identify security objectives for these devices, enabling jurisdictions to more easily select and purchase secure devices and industry to design and build more secure public safety devices.

Keywords

cybersecurity; first responders; internet of things; IoT; mobile security; public safety; wearables.

Acknowledgments

First and foremost, the authors wish to gratefully acknowledge the contributions of the public safety professionals offering their time and rich expertise to this study. Additionally, information gleaned from the Association of Public-Safety Communications Officials (APCO), specifically Mark Reddish, was invaluable. The authors also would like to thank their colleagues who reviewed drafts of this document and contributed to its technical content including John Beltz, Michael Ogata, Andrew Regenscheid, and Nelson Hastings of NIST; Vincent Sritapan of DHS S&T.

Audience

This document is intended for those acquiring mobile devices and wearables for deployment in public safety scenarios. This document may also be useful for those designing public safety smartphones, tablets, and wearable devices.

Table of Contents

List of Tables

List of Figures

List of Appendices

1 Introduction

The Middle Class Tax Relief and Job Creation Act of 2012 created the First Responder Network Authority (FirstNet), an independent agency under the Department of Commerce's National Telecommunications and Information Administration (NTIA) [1]. FirstNet has a mission to develop, build, and operate the country's first Nationwide Public Safety Broadband Network (NPSBN). The NPSBN will enable first responders to begin using modern communications devices for public safety activities. These devices will replace or complement land mobile radio (LMR) handsets, and entirely new categories of devices will be introduced. This influx of new technology will fundamentally alter how first responders communicate and access public safety resources and data. While these new communications technologies will undoubtedly assist first responders, they will also need to be secured against threats to device and communication security to which members of public safety may be unaccustomed.

First responders will not only need modern voice communication technology but also sensors and other wearable devices to properly perform their duties. Wearables are a subset of Internet of Things (IoT) technology physically affixed to a human's body or clothing. Often a dedicated device with a single purpose, wearables and sensors can provide beneficial functions such as authentication, heart rate monitoring, video recording, hands-free communication, or location tracking. Wearables can provide critical information and improved usability, all without interfering with the first responder's typical workflow. These devices also bring unique threats that the larger security community is still learning how to properly address. Securing mobile devices and wearables targeted for public safety will keep first responders and their data secure.

In addition to utilizing the NPSBN, these mobile devices and wearables can be part of a network dedicated to an individual, otherwise known as a Personal Area Network (PAN). PANs can be used as a communications network to transmit information between public safety smartphones, tablets, sensors, and wearable devices. Often operating within a short physical radius, PANs use a completely different set of wireless networking protocols than cellular or LMR devices such as WiFi or Bluetooth. The security interactions between these devices and protocols need to be understood to ensure public safety activities are not adversely affected.

1.1 Purpose

Public safety has unique needs regarding the security of their mobile devices and wearable technology. First Responders use this technology under unique stress, and devices must be specifically designed to operate in those conditions. Commercial-off-the-shelf (COTS) devices may not be able to withstand extreme temperatures and other elements of hazardous environments. Public safety also handles more sensitive data (e.g., patient information, law enforcement data) than the typical commercial user. The overarching goal of this work is to identify security objectives for public safety mobile and wearable devices, enabling jurisdictions to more easily select and purchase secure devices and device manufacturers to design and develop them. The specific contributions of this document include the:

- Collection of public safety use cases, which are then analyzed for relevant cybersecurity considerations

- Identification of previous attacks to similar public safety systems to inform this effort
- Threat modeling activities to understand the necessary technical security capabilities of public safety devices
- Development of security objectives

Established security objectives can provide a reference for those developing public safety communication devices and wearables. Likewise, those within a public safety jurisdiction charged with purchasing equipment can use these objectives when making purchase decisions.

1.2 Scope

This research effort focuses primarily on public safety mobile and wearable devices and the communication between those devices. For instance, when securing broadband networks, the management and operation of cellular networks are out of scope. While an entire class of devices exists under the IoT umbrella, this document solely focuses on wearable IoT devices that may be used by public safety. Additionally, mobile applications that ship with a public safety smartphone are considered in scope as they are often required to perform typical public safety activities, such as voice communication. Backend services and the communication paths utilized by these mobile applications (to include data transmission from an application to supporting infrastructure) are in scope. Finally, first responders work in a variety of disciplines. This Interagency Report (IR) is focused on the fire service, EMS, and law enforcement.

1.3 Previous Work

Readers are highly encouraged to first read NISTIR 8080, *Usability and Security Considerations for Public Safety Mobile Authentication* [11] and NISTIR 8135, *Identifying and Categorizing Data Types for Public Safety Mobile Applications* [2]. NISTIR 8080 analyzes usability issues pertaining to the use of various authentication technologies, including wearable devices. Interviews were conducted to understand the context for how these wearable devices can be used by public safety professionals, and that information is included within the report. NISTIR 8135 explores the categorization of public safety information types for public safety applications, obtained through a public workshop. It is also useful as a foundation for the threat analysis activities explored later in this document.

1.4 Document Structure

The document is organized into the following major sections:

- Section 2 provides an overview of LMR, LTE, and wearable technology
- Section 3 outlines the methodology used for this research
- Section 4 reviews applicable guidance and programs affecting public safety technology
- Section 5 details use cases for public safety mobile devices and wearables
- Section 6 identifies known threats to applicable public safety systems
- Section 7 defines a threat analysis of mobile and wearable devices
- Section 8 explores security objectives for public safety technology
- Section 9 contains conclusions and explores future research areas

The document also contains appendices with supporting material:

- Appendix A defines selected acronyms and abbreviations used in this publication
- Appendix B contains a list of references used in the development of this document

1.5 Document Conventions

The term *mobile device* is used to refer to a modern smartphone running a full-fledged operating system (OS). Please refer to *NIST Special Publications (SP) 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise* for additional information on defining mobility [4]. Mobile devices generally have cellular service, but not always. *Tablets* are traditionally larger than mobile devices, run a full-fledged OS, and are typically assumed to lack cellular service unless otherwise noted. The term *LMR handset* refers to a handheld communication device broadly used by public safety officials in the field today. LMR handsets do not generally have cellular capabilities. The term *wearable*, or *wearable device*, refers to a small device that may or may not have a full-fledged OS. Wearables are generally assumed to lack cellular service and rely on short-range wireless protocols like WiFi or Bluetooth, but this is not always the case.

2 Technology Overview

The following section describes the foundational technologies reviewed throughout this effort.

2.1 Land Mobile Radio Technology

Public safety has employed LMR technology for decades. The two-way radios can operate in vehicles, referred to as “mobile radios,” or on foot, known as “portable radios.” LMR systems typically operate in three bands—very high frequency (VHF) operating at 136-174 megahertz (MHz); ultra-high frequency (UHF) operating at 380-520 MHz; and the 700/800 MHz band operating in four segments: 764-776 MHz, 794-806 MHz, 806-824 MHz, and 851-870 MHz. Each band has different propagation characteristics, with VHF providing less attenuation over a distance and improved propagation in mountainous environments compared to the other two bands. This makes the VHF band ideal for use in rural environments, but it suffers in urban environments due to poor penetration depth. In contrast, UHF and the 700-800 MHz are well-suited for to high-noise city environments but suffer at long distances. Compared to cellular networks, LMR user equipment typically have higher output power and thus improved range, with two to five watts in portable radios and 15-50 watts in mobile radios.

Several co-existing LMR technologies have developed over time. They include three different general types of modulation—analog, APCO Project 25 (P25) [41], and non-P25 Digital. Each modulation scheme can support three different system architectures: direct mode (sometimes referred to as “simplex”), conventional, and trunked. Within the public safety community, analog and P25 modulation schemes are the most common. Analog radio systems typically use frequency modulation (FM) and often transmit unencrypted. The P25 digital modulation scheme allows for data to be transmitted along with the voice channel, which can support encryption to protect radio communications when necessary. When implemented, this voice and data encryption can protect a channel, to be used within a station, a department, or within inter-jurisdiction operations (e.g. mutual aid calls). P25 also supports changing encryption keys in the field using over-the-air rekeying (OTAR). The security aspects of P25 and other associated issues have been researched and documented and are out of scope for this document [20].

Direct mode allows for communication from one user directly to another user or group of users without the aid of any outside network. This is common with larger incidents where many public safety users are in close proximity and would be impeding incident and agency operations by using the repeater system infrastructure. Conventional LMR systems operate similarly to direct mode but use repeating infrastructure to increase the range to a much larger area. The repeater operates at a single frequency pair (i.e., one transmits frequency and one receives frequency) to relay a single talk group. This architecture requires multiple sets of repeaters at varying frequencies per site to support multiple talk groups. These are typically used in smaller jurisdictions and rural environments where one or more departments within a single jurisdiction have a relatively small amount of traffic.

Trunked systems have a control channel and multiple traffic channels, allowing for a large number of talk groups. When a user transmits, the control channel assigns an available open traffic channel to the transmitting user. The control channel handles user equipment registration with the trunked system as well. Some trunked systems are implemented as trunked networks.

One example is a state-wide trunked radio network which implements a set of talk groups across many trunked repeaters that are tied together. These systems allow for more interoperability over a large geographical area without reprogramming the user equipment between jurisdictions and operate like cellular systems using time-division multiple access (TDMA).

2.2 Cellular Technology

A cellular network is a wireless network with a distributed coverage area made up of cellular sites housing radio equipment (i.e., base stations). These base stations are often owned and operated by a wireless telecommunications company. The 3rd Generation Partnership Project (3GPP) is a worldwide standards development organization focused on cellular technology, including 3rd Generation (3G) universal mobile telecommunication system (UMTS) and 4th Generation (4G) LTE technologies. LTE networks are deployed across the globe, and installations continue to increase as the demand for high-speed mobile networks is constantly rising. 3GPP defines a number of high-level goals for LTE systems to meet, including:

- Provide increased data speeds with decreased latency,
- Improve upon the security foundations of previous cellular systems,
- Support interoperability between current and next generation cellular systems and other data networks,
- Improve system performance while maintaining current quality of service, and
- Maintain interoperability with legacy systems [3].

The forthcoming NPSBN will rely upon LTE cellular technology, although 2nd Generation (2G) and 3G cellular technologies may also be used for fallback. 3GPP is also working to standardize specific functions for public safety, such as mission critical voice (MCV) [44]. In the United States, 20 MHz of spectrum is allocated directly to public safety, known as Band 14. The NPSBN will utilize this spectrum with LTE technology. For information on the security of LTE, see NIST SP 800-187, *Guide to LTE Security* [9]. It is of note that 3GPP's newest releases include 5G technology, with deployments rapidly approaching.

Cellular mobile devices are commonly used in public safety scenarios, and the NPSBN will promote a dramatic increase in this usage. They may be issued as a dedicated enterprise device or used in a more *ad hoc* fashion through bring your own device (BYOD) and department stipends. These devices may ship with mobile applications specifically written for the first responder community. Public safety devices often have custom hardware interfaces and additional modifications to make them significantly more ruggedized and public safety user-friendly than typical COTS smartphones and mobile devices.

2.3 Wearable Technology

A wearable is an IoT device that is worn on the body or as an accessory. Wearables are often single-purpose embedded systems collecting data from a set of sensors built into the device. The sensors can collect a wide variety of information, such as the body's current thermal temperature, cardiovascular activity, or GPS location. In some instances, such as smartwatches, wearables can run applications quite similar to mobile applications. These devices may or may not run a traditional OS with modern security features enabled. In fact, many sensor-based devices may not even run what could be considered a traditional OS.

Although wearable devices may have a physical interface, they generally communicate wirelessly. Many wireless protocols can be used to transmit wearable data, including WiFi, various types of Bluetooth, and cellular. WiFi and Bluetooth use the industrial, scientific and medical (ISM) band operating at 2.4 Gigahertz (GHz). WiFi can also operate at 5 GHz. Wearables with cellular service are available with 2G, 3G, 4G, or some other type of cellular connectivity.

As with many IoT devices, wearable technology is still in its infancy. It is popular in the consumer world with the production of devices such as smartwatches, fitness trackers, and Bluetooth headsets. A wearable may transmit information back to a central control unit without direct user interaction. This automation could be convenient for public safety because it will not disrupt their focus on the situation at hand. Although uncommon, some wearables are becoming standalone devices with dedicated cellular connections.

Once configured, wearables are often managed by a desktop or smartphone application. Wearables most commonly communicate with a mobile device via a vendor-provided application (e.g., Apples' *Watch* application or the *Fitbit* mobile application). These applications add an additional layer of attack surface. The security posture of these applications may have a major impact on security. Figure 1 shows how various wearables may interact with a public safety professional.

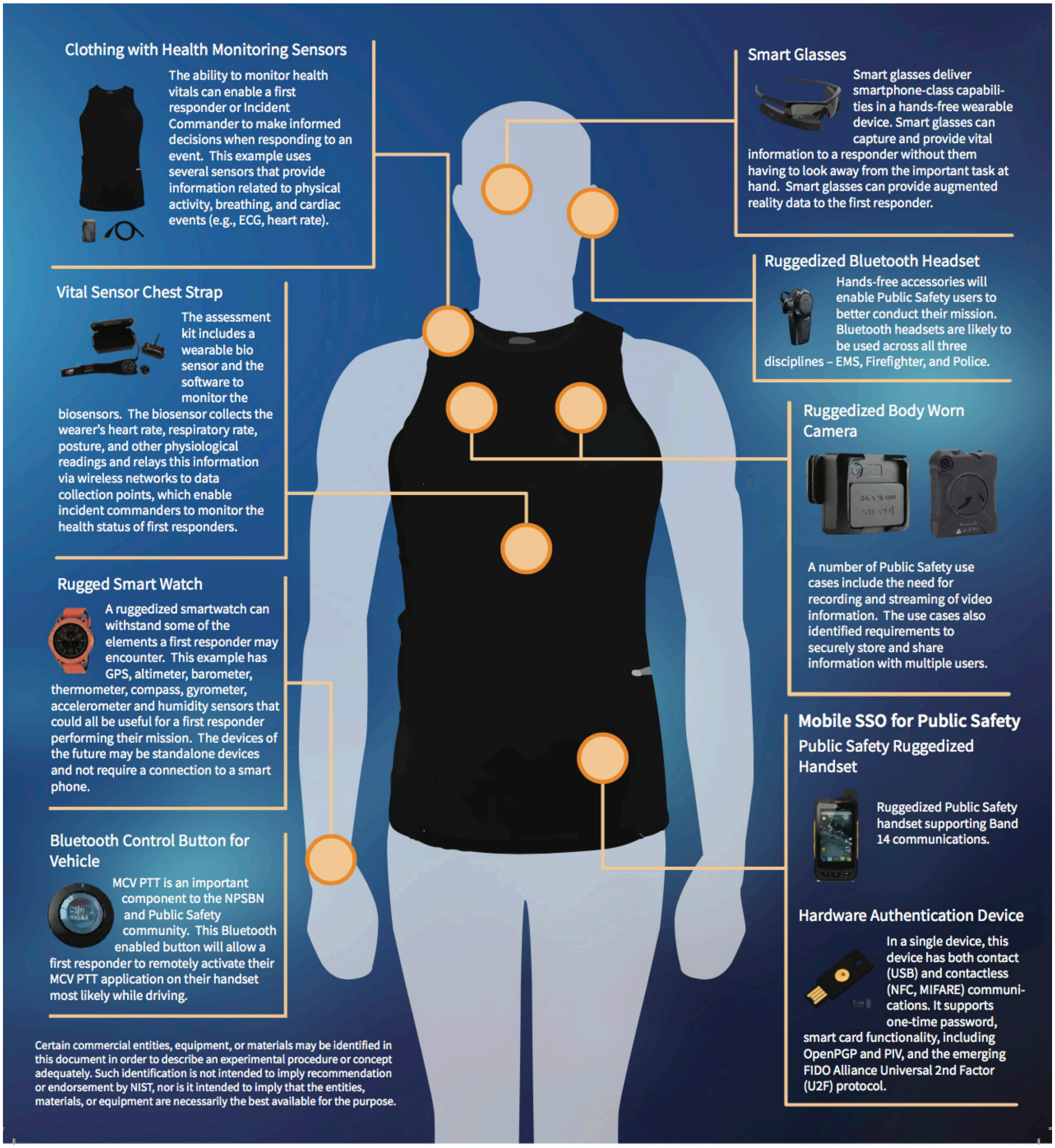

Figure 1 - Examples of Public Safety Wearables

One of the most current and widely used applications of wearable technology are body cameras for law enforcement. Body cameras are used across the United States to record audio and video of an officer's daily duties. These recordings have proven to be vital in providing evidence in court cases. Wireless headsets are another popular wearable in use today by public safety, providing a speaker and microphone for voice communication.

Wearable devices can also provide situational awareness through the data collected from the sensors, such as an individual's GPS location, heart rate, and other health data. This could be useful when, for instance, monitoring the status of firefighters responding to a fire emergency. If a firefighter's heart rate slows or stops, or if other tracked vital signs indicate a problem, the wearable can send a warning to the fire chief or Incident Commander with that firefighter's status and location. In contrast, wearable devices used by EMS responders can be used on both the emergency medical technician (EMT) and on patients. A vital sign wearable can report blood pressure/blood sugar levels and other vital signs back to the hospital where a doctor can provide real-time assistance to the responder about how to provide proper treatment to a patient.

3 Related Standards and Guidance

The public safety users interviewed were asked where they obtain security information for mobile devices, wearables, and LMRs. Federal users cited internal policy while many state and local users cited organizations including, but not limited to, the various components of the Department of Homeland Security (DHS), NIST, FirstNet Authority, and the National Public Safety Telecommunications Council (NPSTC).

3.1 Association of Public-Safety Communications Officials

The Association of Public Safety Communications Officials (APCO) International is an established industry organization of public safety communications professionals from a variety of public safety disciplines, including law enforcement, fire service, and EMS [41]. APCO International assists public safety practitioners by providing professional development, technical assistance, advocacy, training, and outreach services. The organization also runs an online application community known as AppComm—a central repository of mobile apps dedicated to public safety and its use cases [43].

3.2 Department of Homeland Security

The Department of Homeland Security (DHS) oversees several programs that promulgate security guidance related to public safety and, more broadly, the use of mobile devices. The United States Computer Emergency Response Team (US CERT), a program under the DHS Cybersecurity and Infrastructure Security Agency (CISA), creates general guidance for mobile device security [49]. This guidance is intended for consumer and commercial users rather than public safety users but can nonetheless be valuable in securing mobile devices. DHS also manages SAFECOM [50], a program which provides guidance for inter-agency and inter-jurisdiction procedures and best practices and offers grants for enhancing public safety communications equipment. State and local public safety entities often use SAFECOM guidance when developing public safety communications systems since it must be adhered to when applying for SAFECOM grants [51].

The DHS Office of Emergency Communications oversees the DHS Science and Technology Directorate and thus the First Responders Group (FRG), which publishes research and guidance on topic-specific public safety communications applications [52]. This includes reliability and security applications using various public safety communications systems and next-generation first responder technologies.

At a high level, DHS publishes two categories of guidance with regard to mobile device security: internal cybersecurity policy and published reports and recommendations on cybersecurity best practices. The DHS Office of the Chief Information Officer (OCIO) uses the DHS 4300A Sensitive Systems Handbook [42] to inform department-wide policy on information systems security. Specific guidance for mobile devices and wearables can be found within the handbook's Attachment Q1 Sensitive Wireless Systems, Attachment Q2 Mobile Devices, and Attachment Q6 Bluetooth Security.

3.3 FirstNet Public Safety Advisory Committee (PSAC)

The FirstNet Public Safety Advisory Committee (PSAC) is comprised of public safety professionals who generate feedback and guidance to assist in the development of the NPSBN. Such guidance includes PSAC's *Use Cases for Interfaces, Applications, and Capabilities for the NPSBN* [14]. Many public safety leaders refer to PSAC when developing their own policies and recommendations with regards to mobile applications and mobile device usage and to determine how their agencies will be affected by the transition to FirstNet.

3.4 National Public Safety Telecommunications Council

The National Public Safety Telecommunications Council (NPSTC) creates guidance on the research and development of public safety technologies for efforts like FirstNet and the Public Safety Communications Research (PSCR) program. Such guidance includes use cases, reports on the effectiveness of interoperability standards, and recommendations for implementing standards including, but not limited to, system interoperability, communication system encryption, and channel naming conventions [53].

3.5 Public Safety Communications Research

The PSCR program is run jointly by NTIA and NIST and overseen by the United States Department of Commerce. PSCR conducts research, development, testing, and evaluation of communication technologies to improve nationwide public safety. In 2013, PSCR began cybersecurity research efforts related to public safety communications including public safety mobile application security [54].

3.6 NIST Information Technology Laboratory

NIST produces numerous security standards and guidance documents with regard to mobile device security, many of which are used to develop department and agency-level policies and guidance within the Federal Government. These are found in the NIST SP 800 series of publications.

3.7 National Telecommunications and Information Administration

NTIA has several offices that produce public safety-related guidance. The Office of Public Safety Communications (OPSC) manages grants for state and public safety entities to create interoperable systems and for preparation for FirstNet. The Office of Spectrum Management (OSM) provides guidance for federal users, particularly with regard to spectrum allocation and usage [55]. This includes requirements and best practices for frequency usage and communications system design. Additionally, NTIA’s Institute for Telecommunication Sciences (ITS) provides best practices for communications system design and implementation, as well as issues found through its technical research and publications, at times in conjunction with NIST PSCR [56].

4 Study Methodology

This section provides an overview of the methodology used to conduct this study. Security objectives for public safety mobile devices and wearables were identified and developed in consultation with industry members and the greater public safety community. This was accomplished through three main tasks: preliminary research, public safety input, and a collective security analysis, all of which are described in detail below.

4.1 Preliminary Research

PSCR engineers began by studying the use cases of mobile devices and wearables in the public safety space as well as the current security threats to those systems. This research enabled them to analyze how such threats impact daily activities. PSCR engineers reviewed existing documentation of public safety use cases and cyberattacks—particularly attacks on mobile devices and wearables—all of which were publicly available or made so by the public safety community. They then selected and modified certain use cases to ensure relevancy to the scope of security of public safety mobile devices and wearables.

4.2 Public Safety Input

Input from the public safety community was essential to identifying and understanding relevant security concerns. PSCR engineers conducted interviews with federal government personnel working on public safety communications as well as public safety officials who operate and maintain LMR and cellular equipment for EMS, fire service, and law enforcement. During the interviews, PSCR engineers asked each of the interviewees a set of questions and received feedback, which has been essential to the final security analysis and identification of security objectives.

4.3 Security Analysis and Objectives Development

PSCR engineers used the preliminary research and input received from public safety practitioners to perform a threat analysis and create a threat event list. A modified version of NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [57] informed the risk analysis methodology used to analyze each threat event, including the vulnerability, threat sources, security category, likelihood, and impact. Based on this analysis, PSCR engineers developed a list of security objectives and their relevance to public safety, which are described in detail in Section 8.

5 Use Cases for Public Safety Mobile and Wearable Device Security

The purpose of this section is to document a set of use cases as part of a foundation for understanding the necessary security capabilities that first responders need for their smartphones, tablets, and wearables.

5.1 Use Case Development Methodology

To develop these use cases, PSCR identified, surveyed, and analyzed previously developed use cases from reputable public safety organizations. These use cases formed the foundation for this effort. Where necessary, PSCR modified and combined use cases to fit within the scope of security on public safety mobile devices and wearables. Below are short descriptions of the references used to develop this document.

Public Safety Advisory Committee, 2014 - Use Cases for Interfaces, Applications, and Capabilities for the Nationwide Public Safety Broadband Network [14]
This document was a collaborative effort between PSAC and NPSTC and submitted to FirstNet. It defined features and functionalities of solutions for usage on the NPSBN by public safety. The use cases within this document were developed for interfaces, applications, and other capabilities that would utilize the NPSBN.

National Public Safety Telecommunications Council, 2015 - Priority and Quality of Service in the Nationwide Public Safety Broadband Network [15]
This document was developed by NPSTC's Priority and Quality of Service (PQoS) Working Group. It focused on public safety needs with regards to PQoS on the NPSBN. This document also established requirements for the Nationwide Priority and QoS Framework.

SAFECOM Program/DHS, 2006 - Statements of Requirements for Public Safety Wireless Communications & Interoperability [16]
This document was developed by the SAFECOM program, which was created by the Department of Homeland Security's Office of Interoperability and Compatibility and received contributions from public safety practitioners and government organizations. It is a statement of requirements (SoR) focused on the communications and information sharing needs of first responders.

FirstNet, 2015 - Appendix C-9 Nationwide Public Safety Broadband Network Use Case Definitions [17]
This document was developed to provide a collection of use cases for the NPSBN to meet FirstNet's objectives. The uses cases were based on another of FirstNet's documents, Appendix C-7 Operational Architecture.

5.2 Use Case Structure

The use cases were divided into three sections: mobile devices, wearables, and applications. The mobile device use cases include scenarios which involve communication devices such as LMRs, mobile phones, and tablets. The wearable use cases focus on peripheral devices used to gather information (e.g., sensors, cameras, scanners). The application use cases include the software on the devices used to gather, process, and/or transmit information.

Each use case utilizes the following format:

- Title: listed as a section header
- Source: the document used to develop the use case, with appropriate references to the use case or section number from that document
- Technology: the necessary hardware and/or software
- Description: the public safety response scenario
- Concerns: the security concerns identified within the scenario

5.3 Mobile Device Use Cases

5.3.1 Mobile Information Collection and Sharing

Source: PSAC #26
Technology: public safety mobile device, backend storage location, virtual private network (VPN)

Description
While in the field, a police officer is utilizing their mobile device to record and capture pertinent information for a missing person's case. This case information is relayed back to their department's data storage facility to be reviewed by investigators, supervisors, and other command staff. The officer uses their mobile device to share specific details of the missing person's information to responders, public, and media, which may lead to a quicker resolution of the incident.

Security Concerns
The data stored on the officer's mobile device and the backend storage facility may be unencrypted. The data in transit for the data transfer to the backend storage location may be unencrypted if a VPN is not utilized. The unencrypted data allows for easy access of information by unauthorized users. Lack of network availability could delay the officer from quickly transferring the missing person's information to the necessary parties and media outlets.

5.3.2 Shared Equipment with Multiple Users

Source: NPSTC #2.7, SAFECOM 3.3.1, FirstNet 4.8.4
Technology: public safety mobile device, device-side user isolation technology, single sign-on services

Description
A police officer selects a device from a charging station. Although this device is different from the device the officer used yesterday, the officer proceeds to log into the device. After login, the device is automatically configured with the officer's Quality of Service, Priority, and Preemption (QPP) information, and public safety mobile applications are configured with the appropriate settings.

Security Concerns

The officer may have unauthorized access to sensitive information that was authorized for a previous user. Additionally, accidentally collected PII may be exposed, and QPP values may be incorrectly assigned (e.g., higher priority incorrectly assigned to a lower priority user). Location data and health information may also be incorrectly associated with the previous user. The audit logs for the device or applications may be inaccurate. Availability concerns exist if the single sign-on (SSO) service goes down and the device needs to quickly be used for an emergency.

5.3.3 Gathering and Processing Biometric Information

Source: DHS Mobility Use Cases
Technology: public safety mobile device, biometric peripheral, VPN service, public safety database

Description

A law enforcement officer needs to identify an individual in a remote area. They use a wearable sensor to capture biometrics to facilitate the identification of the user. The information is transmitted to HQ for processing. The officer receives the results, which provide improved situational awareness and enable an informed action. Depending on coverage, the device may operate in limited offline mode, over 802.11 wireless, LTE, or satellite communications.

Security Concerns

Data at rest protection for the information on the officer's mobile device and the associated databases storing the biometric information is important to ensure that only authorized officials receive the information. Data in transit protection for the biometric information is also important and could be provided by encrypting the data at the application level and encrypting the communications path (i.e., encrypted data and encrypted tunnel). Encrypting this data can protect against unauthorized extraction or modification of the data in transit. In addition to authenticating to the mobile device, the officer must be strongly authenticated to the applications and backend public safety databases.

5.3.4 BYOD User

Source: PSCR Security
Technology: MDM/EMM/UEM, public safety mobile device, personal public safety mobile device, Bluetooth headset

Description

A firefighter is responding to an emergency and utilizing their fully functional PSBN device. Without warning, the PSBN device ceases to function, and the firefighter is unable to determine the cause of the malfunction or put the device in an operational state. To continue their duties, the firefighter uses their personal mobile device to conduct needed tasks, including downloading and logging into public safety applications.

Security Concerns

The primary concern is that the firefighter needs to carry out their duties with a strong emphasis on voice communication. The firefighter may be using an audio headset or other Bluetooth push-to-talk (PTT) peripheral that may not be paired with their personal device. Another availability issue is whether or not the necessary applications can be quickly configured and/or accessed on their personal device. Finally, since their personal device is not professionally managed, unpatched OS or application vulnerabilities may exist, putting sensitive information at risk.

5.3.5 BYOD - VDI on Tablet/Mobile Device

Source: DHS Mobility Use Cases
Technology: VDI application, backend VDI infrastructure, public safety mobile device

Description

A first responder requires access to disaster-specific information. The individual uses their personal tablet to access agency applications through a virtual desktop infrastructure (VDI). The VDI application is removed at the end of the disaster.

Security Concerns

Any user with access to the personal tablet may also have unauthorized access to the agency applications through the VDI. The connection between the VDI mobile application and the backend VDI infrastructure should require authentication and be confidentiality protected. The tablet should be free of known vulnerabilities and malware. No incident data should be stored on the device.

5.3.6 Lost or Stolen Device

Source: PSCR Security
Technology: Enterprise Mobility Management (EMM), public safety mobile device

Description

Two police officers are patrolling their assigned area on foot, searching for a person of interest. One officer notices an individual and begins to actively pursue. During the chase, the officer loses their mobile device. Once the suspect is apprehended, the officer realizes their phone is no longer on their person and subsequently notifies the police department's device manager of the device loss.

Security Concerns

An unauthorized user may find the device and attempt to access the stored information. Depending on the how the device performs lockscreen authentication, an unauthorized user may be able to view sensitive information. If the device is configured to push notifications to the device lockscreen, an unauthorized user can access texts or other data regarding sensitive public safety matters. If the individual who finds the device puts it into a Faraday bag, the police department's device manager may be unable to physically locate or remotely wipe the device. In this case, pertinent data to a case or other important data stored solely on the device will be lost.

5.3.7 Communication Between Neighboring Jurisdictions

Source: PSCR Security Group
Technology: public safety mobile device, encryption, dispatch
Description
Police officers respond to an incident that results in an on-foot pursuit. The chase takes them across county lines where they request assistance from the local police department. The counties have implemented encryption on their devices; however, an open channel for dispatch is accessible. The officers switch to the open channel and relay their needs. Local law enforcement can receive the transmission and assist in pursuing the suspect.

Security Concerns
Neighboring jurisdictions may be unable to communicate if encryption keys are not shared before an incident occurs. Additionally, a jamming device can obscure the lines of communication by disrupting the device's connection to cellphone towers in the area. Even if communication is available, the confidentiality of the information may be compromised. A rogue base station can perform a man-in-the middle-attack and secretly intercept data sent between a device and a cell tower. This could potentially allow for eavesdropping, and collected information may be used in a malicious manner.

5.4 Wearable Device Use Cases

5.4.1 Wearable Integrated Sensor Technology

Source: PSAC #12 / NPSTC 2.12
Technology: wearable health sensor, backend server, public safety mobile device

Description
An EMS employee in a hazardous environment is utilizing multiple wearable devices and sensors to monitor their health status (e.g., blood pressure, heart rate, respiration, temperature, blood oxygen, head orientation, external temperature, and environment information, including air quality readings) and enable voice communication. All connected to a smartphone creating a PAN, the wearable sensors are preconfigured with location tracking and health monitoring. This information is reported in real-time to the Incident Commander and dispatch center. The Incident Commander can monitor the location of all their EMS employees deployed to the hazardous environment via their tablets.

Security Concerns
Confidentiality protection concerns exist for the wearable devices transmitting data to the smartphone and then to the Incident Commander. If the wireless communication path is jammed, the Incident Commander is no longer able to communicate over voice or monitor the location and vitals of EMS employees working in the hazardous environment. If a malicious actor is able to spoof sensor feeds, then an inappropriate or incorrect response may be issued by the Incident Commander.

5.4.2 Bodycam

Source: PSCR Security Group
Technology: body camera, cloud storage platform, public safety mobile device

Description
A law enforcement officer responds to an emergency. The officer is wearing a body camera which records information at the scene of the emergency and streams the recording to a cloud platform. The video stream is accessible to privileged users who are authorized to review the content. The recording is later permanently placed in the cloud archive.

Security Concerns
The bodycam footage should be encrypted when streamed within the PAN (wearable camera to the mobile device), to the cloud storage platform, or onto any other information system. Only authenticated users should be able to access the bodycam footage, which should also be encrypted in storage. The cloud storage platform is secure and backs up the bodycam footage. Availability concerns exist if the bodycam loses battery.

5.4.3 Patient Monitor

Source: PSAC #17
Technology: wireless vital signs monitor, laptop, GPS constellation

Description
A first responder places a wearable sensor on the exposed skin of each patient at the scene of a mass casualty incident (MCI). The sensor checks several physiological signs (e.g., blood pressure, heart rate, respiratory rate, blood oxygen) and sends the vital signs along with GPS coordinates to a laptop via Wi-Fi. This laptop displays a color-coded dot indicating the patient's condition and their position relative to other patient "dots" on the screen. This information can also be transmitted to local hospitals.

Security Concerns
Confidentiality protection concerns exist for the wearable sensor transmitting data to the laptop, with an emphasis on protecting the patient’s medical data and ensuring compliance with Health Insurance Portability and Accountability Act (HIPAA). The information also needs to be protected if it is sent to a local hospital. If the data from the sensor is spoofed or modified, the medical professional observing the readings may perform a wrong or unnecessary medical treatment or fail to provide treatment when it is needed. Therefore, the data integrity needs to be protected and appropriately authenticated. If the PAN wireless communication path is jammed, the medical professional can presumably use alternative methods to obtain the necessary information.

5.5 Mobile Application Use Cases

5.5.1 Application Dependent Devices

Source: PSCR Security Group
Technology: public safety mobile device, wearables, public safety vendor application

Description
A large-scale fire event is in progress, and a Fire Chief has deployed firefighters to cover the emergency. The firefighters have wearable location sensors on their uniforms which communicate with an application on the Fire Chief's mobile device and allow the Fire Chief to monitor the location of each firefighter.

Security Concerns
The security posture of the applications used have a major impact on the security of public safety officials. The application described in this use case receives the firefighters' location information, which could be dangerous if the data is received by a malicious actor. It is important to ensure that the data cannot be intercepted and is only routed to the necessary endpoints.

5.5.2 Sharing of CAD Information via Mobile App

Source: PSAC #39
Technology: public safety mobile device, CAD application, backend server

Description
Prior to arriving on a scene, a first responder can receive CAD dispatch information on their mobile device via a CAD application. The application can provide known patient information and the state of the emergency. The first responder may be better physically and mentally prepared for the emergency with the CAD application.

Security Concerns
The transmission of unencrypted CAD dispatch information may allow malicious users sniffing the communications path to obtain sensitive public safety information. Additionally, concerns over breaching PII and medical information exist if known patient information is transmitted.

5.5.3 Patient Tracker

Source: PSAC #29
Technology: public safety mobile device, mobile patient mobile application, smart medical bracelet, receiving hospital information system

Description
A large-scale incident has occurred, and there are mass casualties. First responders are at the emergency site providing initial care and transporting patients to various hospitals in the area. Each patient is given a medical wrist band, which is scanned into a mobile application. The application uploads basic patient information to dispatch, the emergency operations center

(EOC), and receiving hospitals. This application is important when monitoring each patient's location at their current hospital.

Security Concerns

Any handling of patient information must be compliant with HIPAA. The patient data uploaded from the mobile application should be protected from eavesdropping through encryption and integrity protection, likely via a VPN. To avoid unauthorized access, the session between the mobile application and the hospital information system should be authenticated.

5.5.4 Electronic Patient Care Recording (EPCR) application

Source: PSAC #32, SAFECOM 3.2.2
Technology: EPCR application, public safety mobile device, backend server

Description

While assisting a patient, an EMS employee is recording patient information into an EPCR application. Basic patient information and any treatment given at the scene of the emergency are recorded in the EPCR application. This information is then sent to the local hospital and physician who will be receiving the patient.

Security Concerns

Vulnerabilities may exist in the mobile EPCR application, allowing unauthorized external parties to access or modify patient medical information. Medical information stored on the phone and then sent to the backend may not be cryptographically protected. The backend database may not require authentication, allowing unauthorized inserts, modifications, and deletions. Concerns over violating HIPAA exist.

5.5.5 EMS Database

Source: PSAC #34
Technology: public safety mobile device, backend server, EMS database application

Description

An EMS first responder is analyzing drugs at the scene of an overdose. Using a mobile device, the first responder takes a picture of the drugs and submits the photos to an EMS application that compares the photos to medications within a database. Once a match is found, the application provides suggested treatment. Using the EMS database application, the first responder can also look up EMS protocols for the proper dosage of specific medications as well as a patient's medical records.

Security Concerns

The application may not encrypt the images sent to the external database, allowing others to observe the information at the scene and obtain a detailed view of the paramedic's surroundings. The backend database may not require authentication, allowing unauthorized inserts, modifications, and deletions.

5.5.6 Mission Critical Voice (MCV) Application

Source: NPSTC 2.2
Technology: MCV application, public safety mobile device

Description
A large group of first responders is sweeping through a heavily wooded area on a search and rescue mission. One first responder gets separated and lost. The first responder uses a wireless headset to interface with the MCV application on their mobile device to call for assistance.
Security Concerns
The MCV application may not encrypt the data received and/or authenticate the headset to the mobile device. This would allow external parties to listen to voice traffic and transmit false voice traffic by posing as a first responder.

5.5.7 Video Telemedicine Application

Source: NPSTC 2.5
Technology: video telemedicine application, public safety mobile device with camera

Description
A paramedic is at the scene of an emergency and requires extra assistance to care for a patient. The paramedic uses a video application to communicate with a physician for guidance on how to properly treat the patient. The video application gives the physician a visual of the scene to provide accurate assistance to the paramedic.

Security Concerns
The application the paramedic is using may not encrypt the video session, allowing external third parties to observe the conversation and obtain a detailed view of the paramedic's surroundings.

5.5.8 Collect Information through UE Camera

Source: DHS Mobility Use Cases
Technology: public safety mobile device with camera, PDF converter application

Description
A detective travels off-site to access physical records. While reviewing the information, they takes photos of documents with their phone before then launching a mobile application that converts the photos to PDF documents.

Security Concerns
The detective may be using an older device that does not encrypt the device's NAND flash by default. The application may not have appropriate mechanisms enabled to protect the information. Finally, the application may contain vulnerabilities that allow a malicious third party to obtain the photos or PDFs stored on the device.

5.5.9 Push-To-Talk Telemedicine Application

Source: NPSTC 2.11
Technology: push-to-talk (PTT) application, public safety tablet

Description
A paramedic needs additional assistance to treat a patient. The paramedic is unable to establish a video session via their tablet and resorts to using PTT to communicate with a physician for treatment guidance. The PTT application allows the physician to support the paramedic by talking through the proper treatment needed to care for the patient.
Security Concerns
The PTT voice data may be unencrypted, allowing external third parties to listen to the traffic. If unauthenticated users can access the channel, there is an increased chance of collisions on the network. This could result in information loss between the paramedic and the physician. This outcome may also occur if the communication path is intentionally jammed.

5.5.10 Side-loading Application

Source: PSCR Security Group
Technology: laptop, public safety mobile device, unsigned mobile application

Description
A law enforcement officer goes to a neighboring jurisdiction and has a need to share sensitive information. The application necessary to share information is not accessible through any commercial app store. The only way to install the application is to side-load the local jurisdiction’s application onto the neighboring officer’s public safety mobile device. The neighboring officer installs the application and receives the pertinent information.

Security Concerns
Sideloading applications may leave the device vulnerable to mobile malware and other improperly signed code if it is not properly reconfigured after installation. The neighboring officer may need to check with their station’s device manager before installing an unfamiliar application onto a public safety mobile device.

5.5.11 Public Records and Applications

Source: PSCR Security Group
Technology: public safety mobile device, publicly available mobile applications

Description
Records from an arrest in the local area are recorded in mobile applications for citizen awareness. The applications are open to the public as well as to public safety officials. This information is useful in crafting a large operating picture for law enforcement and enables the Incident Commander to allocate the appropriate resources.

Security Concerns

Malicious actors may install these applications to track public safety official's activities. Although the officials' location information is not available in real-time, areas of increased presence may easily be identified.

6 Documented Attacks on Public Safety Systems

Reviewing the security incidents historically imposed on public safety mobile devices provides context and a foundation for assessing next-generation threats and introducing new technology. This section details threat sources, attack types, and publicly known attacks on public safety systems. PSCR engineers provide an overview of the publicly known attacks and map them by threat sources, attack type, and impacted security principle (i.e., confidentiality, availability, and/or integrity).

It should be noted that many attacks on public safety systems are often collected and shared via the Homeland Security Information Network (HSIN). Much of the information contained within the Network is sensitive and cannot be publicly shared.

6.1 Threat Source Type Descriptions

This section will identify and describe types of threat sources in accordance with *NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments* [12]. The threat source types are then generalized to documented attacks cited in succeeding sections.

6.1.1 Adversarial

Abusing public data sources: Combining and analyzing information from multiple public data sources to perform a malicious activity

Eavesdropping: Sniffing traffic on a medium that is not confidentiality protected; the content of communications may be used to perform other malicious activities

Insider threat: An individual with privileged access in an organization who uses such access to pose a threat to the organization

Impersonation: An individual or entity masquerading as another, often trusted party; information or actions are typically requested if the impersonator has sufficient privileges to make the request

Theft: Information or physical items are taken without authorization

Malware: A program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system [46]

Denial of service (DoS): Negatively affecting the availability of an information system or process; similarly, distributed denial of service (DDoS) significantly affects the availability of an information system or resource at scale, such as by flooding a network by simultaneously sending data from various computers

6.1.2 Accidental

Misconfiguration: An unintentional DoS caused when an information system is not utilizing the proper system, application, or user settings

6.1.3 Failure of Controls

Equipment Failure: Occurs when a device is unable to perform its normal activities

6.1.4 Environmental

Natural and man-made disasters: A natural or man-made event which causes damage to physical and computer infrastructure

6.2 Adversarial Attacks

The following are attacks that exemplify a malicious external entity actively exploiting a vulnerability. Each attack identifies with an adversarial threat source.

6.2.1 Malware pre-Installed on police body cameras

The Win32/Conficker.B!inf malware was found pre-installed on the police body camera manufactured by Martel Electronics [21]. Conficker, as it is colloquially known, was one of the most successful malware campaigns ever conducted. On the device itself, Conficker affected battery performance before spreading to other information systems. In the context of public safety, connections were made to other public safety mobile devices, equipment, and backend traditional systems located in headquarters [22]. Much of the evidence surrounding this infection points to a supply chain issue.

Threat Source: Adversarial – Malware
Impact: Availability

6.2.2 Ransomware infecting police surveillance equipment

In 2017, days before the 58th presidential inauguration was held in Washington D.C., approximately 70% of the storage devices used to store footage for the Metropolitan Police Department's video surveillance system were infected with ransomware [24]. The system was unable to function properly, and city officials subsequently took the devices offline from January 12-15, 2017, during which time the ransomware was removed, and the systems were rebooted. Washington, D.C. officials stated that this attack was limited to closed circuit TV systems and did not further affect capital city government networks [23]. It remains unclear how the cameras were initially infected.

Threat Source: Adversarial – Malware
Impact: Availability

6.2.3 Unencrypted police communications

In 2012, public safety officials in Anchorage, Alaska transmitted unencrypted voice traffic suggesting that a high school student had a gun in a classroom. Media outlets tweeted about it before police arrived at the scene and could have potentially compromised the safety of the students, teachers, and public safety officials. This launched a discussion surrounding the benefits and drawbacks of using unencrypted police voice traffic. In 2016, public safety transmissions were taken off the air after a string of robberies in Anchorage. City public officials worried that criminals were using mobile scanner apps to their tactical advantage. For instance, an individual stole a rental car in February 2016 and was quickly arrested. Following the arrest, the officer taking the stolen car in for processing heard a delayed transmission that the officer would be pulling the man over. Anchorage public safety organizations no longer broadcast unencrypted radio traffic [25].

Threat Source: Adversarial – Eavesdropping
Impact: Confidentiality

6.2.4 LMR devices stolen

In April of 2012, teens in Dilworth, Minneapolis came across an unlocked police vehicle and stole the contents, including bulletproof vests, weapons, ammunition, and radios [27]. After transmitting profanity on police frequencies, the teenagers called authorities because the handcuffs were stuck on one of the individuals. The teenagers told the police that the radio was tossed into a lake and was ultimately not recovered.

Threat Source: Adversarial – Theft
Impact: Availability

6.2.5 Reporting fake information and issuing personal threats

In 2016, an individual in Manhattan, New York began routinely broadcasting fake incidents and police shootings on NYPD-only radio frequencies, culminating in targeted threats against a specific police officer [29] [30] [31].

Threat Source: Adversarial – Impersonation
Impact: Integrity

6.2.6 Jamming police transmissions

In 2016, a man in Tampa, Florida was fined $48,000 for using a wireless jamming device in his car during a daily commute. The device was built to disrupt cellular transmissions and routinely affected police voice traffic [32].

Threat Source: Adversarial – Denial of Service
Impact: Availability

6.2.7 Mobile devices unwittingly used to launch an attack

In September 2016, an 18-year-old teenager named Meetkumar Hiteshbhai Desai posted a link to Twitter that was intended to force pop-ups to appear and require users to reboot their devices [33]. Instead, the exploit caused mobile devices to continuously call 9-1-1 and hang up by activating automatic dial services. Over 1,000 Twitter users clicked the link. The attack flooded the PSAP call system and significantly slowed the call center's response rate [34]. Updating the device's firmware would later patch this specific 911 DDoS vulnerability.

Threat Source: Adversarial – Denial of Service
Impact: Availability

6.2.8 Unauthorized access at fire station

In 2014, a former fire rescue division chief in Sioux Falls, South Dakota was convicted of 15 counts of hacking. He unlawfully used department computers to obtain unauthorized access to an email between the city and Fire Captain Michael Gramlick, spreadsheets titled "SWAT callouts," a document titled "paystub," and two photos [35].

Threat Source: Adversarial – Insider Threat
Impact: Confidentiality

6.2.9 Combing and presenting law enforcement information via an app store

The Google Play store hosts a mobile public safety app that can be used by malicious users to track arrests made by law enforcement [37]. The app lists data on individuals who were arrested and jailed, as well as the applicable charges. Other descriptive information about the arrested individuals is also identified.

Threat Source: Adversarial – Abusing public data sources
Impact: Confidentiality

6.3 Structural and environmental incidents

The following is a collection of incidents in which the security of public safety systems was threatened but no malicious entity necessarily exists. These incidents identify with structural threat sources.

6.3.1 Radio failure and interference

During the active shooter incident at Washington's Navy Yard, federal firefighter and police officer radios failed. The presence of multiple mobile command centers and a lack of centralized coordination hampered communication. Devices worked initially, but as emergency responders ventured deeper into the building where the shooting occurred, radios stopped functioning. The Incident Commander inside the building could not communicate with those outside of the building. Individual emergency responders eventually had to use cellphones and other ad hoc communication mechanisms [38].
Threat Source: Structural – Equipment failure
Impact: Availability

6.3.2 Inoperable communications systems

A study conducted by the North Dakota Information and Technology Department in 2014 revealed several reliability issues with the state's radio system, which suffers from coverage issues and dead zones [39].

Threat Source: Structural – Equipment failure
Impact: Availability

6.3.3 Service disruptions to the 911 system

In March 2017, AT&T wireless customers in seven states were unable to reach 911 due to a "service issue" that the Federal Communications Commission is still investigating [40].

Threat Source: Structural – Equipment failure
Impact: Availability

7 Threat Analysis

The following section describes the threat analysis performed for public safety mobile devices and wearables. This information can be used to construct a preliminary threat model for this class of information systems. The methodology used to conduct this analysis is detailed below.

7.1 Threat Analysis Methodology

Each threat listed is considered using the scenario of a medium-sized jurisdiction responding to an emergency. Threats are considered within the context of EMS, fire service, and law enforcement. Characteristics are identified and noted for each threat, all of which are defined below. These characteristics include the threat event, vulnerability, threat source, impact category, likelihood, and severity.

Threat events are divided into two major technology categories: those affecting mobile devices and those affecting wearables, each of which are described in separate sections. Threat events were initially taken from the information contained within the use cases and previously identified attacks sections. All threat events are scoped directly to the mobile and wearable devices, which does not include the networks they are connected to or any backend systems. All threat events are initially presented in the following manner and followed by a detailed description of the threat.

Table 1: Example Threat Event

Threat Event	Vulnerability	Threat Source	Category	Severity	Likelihood
Sensitive information is intercepted as it is relayed to an official source	Lack of confidentiality protection	Adversarial	Confidentiality	EMS: Mod Fire: Low LE: High	Infrequent

A *threat event* is defined as any event or situation with the potential of causing undesirable consequences or impact. For example, the loss of radio communications is a threat event for public safety systems. It is important to note that humans are not the only cause of threat events; natural disasters and equipment failures are potential threat events, particularly to the availability of systems.

A *vulnerability* is a weakness in a process or system. This weakness could reside within a set of procedures, internal control, or system implementation that could be exploited by a threat source. A *threat source* is the adversary intending to exploit a vulnerability or a situation that may accidentally or incidentally exploit a vulnerability. The threat sources used within this analysis are adapted from the list of threat sources defined within NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [12], which include:

Table 2: Modified Threat Source Definitions

Adversarial	Hostile cyber or physical attacks from a malicious individual
Accidental	Human errors of omission or commission from a non-malicious individual
Failure of Controls	Failures of hardware, software, and/or environmental controls
Disaster	Natural and man-made disasters, accidents, and failures beyond the control of the organization

Adversarial or hostile threat sources must have the intent and capabilities to attack the system as well as the ability to target vulnerabilities within the system.

The impact of a threat event is its effect on violating a system's basic security objectives. In many cases, risk assessments and threat analyses provide different impact levels for a given threat depending on what security objective is breeched. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* [19] provides definitions for low, moderate, and high impact levels for each of the security objectives (i.e., confidentiality, integrity, and availability). In the case of public safety systems, threat events may lead to various types of impacts. The impact of some threat events may lead directly to an undesirable information disclosure, while others may lead to a loss of privacy or simply render a communications path unusable. Some threat events may impact multiple jurisdictions, while others may only impact a small number of individuals or systems.

Table 3: Potential Impact Definitions from FIPS 199

Security Objective	Potential Impact		
	Low	Moderate	High
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction; includes ensuring information nonrepudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Availability Ensuring timely and reliable access to and use of information [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Severity is a measure of the effect of a threat event occurrence. For instance, threats that lead to loss of life cause a more severe outcome than risks that require a public safety professional to change their means of communication. This analysis uses a three-tiered qualitative scale to assess the severity of a threat event:

- **High-severity** threat events lead to a loss of human life. Under certain contexts, loss of communication or personal identity can be a high-severity event as it may lead to loss of life.
- **Moderate-severity** threat events have a direct impact on public safety goals, such as threats to law enforcement sensitive information or patient medical information.
- **Low-severity** threat events are other events that could occur during an emergency incident that could pose surmountable problems for public safety personnel. These events do not prevent public safety personnel from performing their duties but do make it more difficult to accomplish their goals. Ancillary effects are also included, such as loss of personal information.

Most threat analyses include an estimate of how likely a given threat event is to occur and negatively impact a system or process, especially in terms of security.

The *likelihood* of occurrence of a threat is how often a threat event is initiated or caused by a threat source. To reflect this idea, our analysis replaces the notion of likelihood of a threat event with the expected number of occurrences of a given threat event in each incident. For some types of failures, occurrence estimates can be determined from publicly reported incidents. Precisely determining the number of occurrences of a threat event is unfeasible. Instead, we categorize threats based on occurrence into the groups shown in the table below, based on groups defined in *NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments [12]*:

Table 4: Modified Threat Occurrence Definitions

Very Low	Error, accident, or act of nature is highly unlikely to occur or occurs less than once every 10 years
Low	Error, accident, or act of nature is unlikely to occur or occurs less than once a year, but more than once every 10 years
Moderate	Error, accident, or act of nature is somewhat likely to occur or occurs between 1-10 times a year
High	Error, accident, or act of nature is highly likely to occur or occurs between 10-100 times a year
Very High	Error, accident, or act of nature is almost certain to occur or occurs more than 100 times a year

7.2 Threats to Public Safety Mobile Devices

The following threats concern the use of public safety mobile devices.

Table 5: Threats to Public Safety Mobile Devices

Threat Event	Vulnerability	Category	Threat Source	Severity	Likelihood
Sensitive information is intercepted from a mobile device	Lack of confidentiality protection or poor cryptography	Confidentiality	Adversarial	EMS: Mod Fire: Low LE: High	High
Accidental disclosure of information via a shared device or resource	Lack of properly implemented access controls	Confidentiality	Accidental	EMS: Low Fire: Low LE: Mod	Mod
Individual accesses information and services via a lost or stolen public safety device	Lack of physical access control, lack of user authentication to device	Confidentiality	Adversarial, Human error	EMS: Mod Fire: Low LE: High	Mod
Pre-installed spyware on device accesses sensitive data	Lack of supply chain controls	Confidentiality	Adversarial	EMS: Mod Fire: Low LE: High	Low
A denial of service or other technical attack, blocks communications	Protocol not designed to withstand jamming attacks, lack of available spectrum	Availability	Adversarial, Accidental	EMS: High Fire: High LE: High	Mod

Structural or architectural issues interference	Radios lack sufficient signal strength to penetrate the environment, public safety personnel operate in enclosed environments	Availability	Failure of controls	EMS: High Fire: High LE: Mod	High
Unreliable communications channel due to interoperability issues	Disparate technology configurations across jurisdictions	Availability	Failure of Controls	EMS: Mod Fire: Mod LE: Mod	Mod
Device failure due to a lack of ruggedization	Device components not rated to handle extreme temperatures, liquid, etc.	Availability	Environmental, Human error	EMS: High Fire: High LE: High	Low
Mobile device is infected with malware, resulting in a loss of sensitive information	Lack of OS and/or application updates exposed device to malicious users	Confidentiality	Adversarial	EMS: Mod Fire: Low LE: High	Mod
Location tracking of a public safety mobile device	Lack of malware detection or application vetting	Confidentiality	Adversarial	EMS: Low Fire: Low LE: High	Mod
Malicious management profile or certificate is installed on a device	Practitioner unknowingly accepts the profile	Confidentiality	Adversarial, Accidental	EMS: Mod Fire: Low LE: High	Low

7.2.1 Sensitive information is intercepted from a mobile device

Threat Description: A malicious entity eavesdropping on public safety traffic during an emergency situation

Vulnerability: Several distinct vulnerabilities could be exploited in this instance. The simplest vulnerability is a lack of encryption for the data path used by the mobile device, including cellular, WiFi, and Bluetooth. Additionally, broken cryptographic algorithms and insufficient key sizes could also be used, which could then be broken in order to access plaintext content of communications.

Threat Source: Adversarial

Likelihood: High
Justification: Police scanner applications are available in most app stores, and commercially available equipment allows individuals to easily listen to unencrypted public safety communications.

Severity - Emergency Medical Service: Moderate Confidentiality Impact
Justification: This information could contain personal details about patients, such as first name, last name, address, insurance information, medical history, and current injuries, all of which is subject to HIPAA regulations. This would be unlikely to result in a loss of human life.

Severity - Fire Service: Low Confidentiality Impact
Justification: An adversary with access to this information would be unlikely to pose a threat to a firefighter's immediate survival of the emergency situation at hand.

Severity - Law Enforcement: High Confidentiality Impact
Justification: The classification of this data depends on the type of incident at hand. The high impact level is assigned because there exists the possibility of loss of life. For instance, sensitive information shared at a crime scene or an undercover officer simply communicating with law enforcement could lead to loss of life. It is of note that much of a law enforcement officer's routine communication is sent securely, making this classification situation-dependent.

Source: Use Case – Mobile Information Collection and Sharing**;** Known Attacks – Unencrypted Police Communications in Anchorage, Alaska

Mitigations:
Cryptography can be used to provide confidentiality protection for public safety communications. Encryption can be implemented by the network to simplify algorithm selection and cryptographic key management issues. Encryption could also be provided by an application, which would then use the network as a simple data transport mechanism. In this instance, if the network is also encrypting traffic, information may be encrypted twice. This may cause lower data throughput but may be necessary for disciplines and situations requiring confidential communications.

7.2.2 Accidental disclosure of information via a shared device or resource

Threat Description: In many cases, public safety practitioners share a pool of available radios. This practice may continue with mobile devices, and an information disclosure could occur if an individual reuse a mobile device and finds themselves already logged into services and resources used by a colleague. For instance, the new user may be able to access pictures taken by the previous user. Currently, there is no convenient or fully functional means of signing out of all applications that are in use.

Vulnerability: This situation allows for a lack of or improperly implemented access controls, including both local and remote authentication. In terms of local authentication, the lack of a lockscreen could allow this information disclosure to occur. For remote authentication, a persistent session that does not log out after a pre-determined period could compromise confidentiality of the data.

Threat Source: Accidental

Likelihood: Moderate
Justification: Users may not regularly log out of personal services, meaning this occurs frequently.

Severity - Emergency Medical Service: Low Confidentiality Impact
Justification: Patient information is unlikely to be exposed in this instance as these databases often require additional levels of authentication.
Severity - Fire Service: Low Confidentiality Impact
Justification: Exposed information is likely to be personal in nature rather than sensitive public safety information.

Severity - Law Enforcement: Moderate Confidentiality Impact
Justification: Mature access controls are already in place for databases that host criminal and other sensitive law enforcement information. Unsecured information here would only be accessed by members of law enforcement and not disclosed to the public, lessoning the impact.

Source: Use Case – Shared Equipment with Multiple Users

Mitigations:
Authenticating a specific user to devices and applications before granting access would be a useful control to prevent this type of data spillage. Some smartphones already contain multi-user functionality that could be extended to accommodate the need to share devices. Further research in this area is being conducted at the National Cybersecurity Center of Excellence (NCCoE).

7.2.3 Individual accesses information and services via a lost or stolen public safety device

Threat Description: Lost or stolen devices can allow potentially malicious individuals to access sensitive public safety information. Even with lockscreen authentication, some public safety information may be exposed. For instance, notifications from cellular services (e.g., text messages, missed calls) or installed apps may be shown on the lockscreen.

Vulnerability: This situation is impacted by the lack of or improperly implemented access controls, including both local and remote authentication. In terms of local authentication, the lack of a lockscreen could allow this information disclosure to occur. For remote authentication, a persistent session that does not log out after a pre-determined period could compromise confidentiality of the data.

Threat Source: Adversarial, Human error

Likelihood: Moderate
Justification: Public safety devices may be lost or stolen with the same frequency as commercial and enterprise devices.

Severity - Emergency Medical Service: Moderate Confidentiality Impact
Justification: Patient information is unlikely to be exposed in this instance as these databases often require additional levels of authentication.

Severity - Fire Service: Low Confidentiality Impact
Justification: PII or other sensitive information is unlikely to be exposed.

Severity - Law Enforcement: High Confidentiality Impact
Justification: The exposed information could be quite sensitive with regard to ongoing emergency incidents.
Source: Use Case – Lost or Stolen Device; Known Attacks – LMR Device Stolen

Mitigations:
Properly configured mobile devices that authenticate users or roles before providing access to sensitive information can prevent unauthorized access. For local authentication, a proximity token could be used. For instance, if an officer's badge contains a proximity token, and their badge is physically separated from the phone, the phone automatically locks and requires further authentication. Other forms of authentication may include biometric or behavioral authentication methods. In terms of mitigations for remote authentication scenarios, time-based session logouts and regular reauthentication may be useful.

7.2.4 Pre-installed spyware on device accesses sensitive data

Threat Description: Spyware or other malware could be installed and shipped with a device, compromising the device before it is even activated or provisioned. Spyware could monitor how the device is used and forward information to a bad actor [7].

Vulnerability: Lack of supply chain mitigations that would ensure that only properly sourced software and hardware are used in the public safety mobile device.

Threat Source: Adversarial nation-state and/or adversarial organization supplier

Likelihood: Low
Justification: Although general malware has been seen beforehand, pre-installed malware designed specifically to affect public safety has not been witnessed.

Severity - Emergency Medical Service: Moderate Confidentiality Impact
Justification: This information could contain personal details about patients, such as first name, last name, address, insurance information, medical history, and current injuries, all of which is subject to HIPAA regulations. This would be unlikely to result in a loss of human life.

Severity - Fire Service: Low Confidentiality Impact
Justification: An adversary with access to this information would be unlikely to pose a threat to a firefighter's immediate survival of the emergency situation at hand.

Severity - Law Enforcement: High Confidentiality Impact
Justification: The classification of this data depends on the type of incident at hand. The high impact level is assigned because there exists the possibility of loss of life. For instance, sensitive information shared at a crime scene or an undercover officer simply communicating with law enforcement could lead to loss of life. It is of note that much of a law enforcement officer's routine communication is sent securely, making this classification situation-dependent.

Source: Known Attacks – Malware Pre-Installed on Police Body Cameras

Mitigations:
Proper consideration of risks associated with the supply chain, especially hardware manufacturers and firmware developers, may assist with ensuring the integrity of the system. This potentially includes purchasing devices from trusted vendors. Applications installed on mobile devices and wearables should be vetted. NIST SP 800-163 can assist with the vetting of mobile applications [45].

7.2.5 A denial of service or other technical attack blocks communications

Threat Description: A variety of technical DoS attacks exist, from exploiting protocol specific vulnerabilities (e.g., WiFi disassociation frames), smart jamming attacks, and less sophisticated spectrum jamming attacks. All of these can occur for any wireless protocol, including Bluetooth, WiFi, and LTE.

Vulnerability: DoS attacks can occur when protocols are not designed to withstand jamming attacks or when there is a lack of available spectrum to use. Many technologies that will be deployed will utilize the already noisy ISM band.

Threat Source: Adversarial, Accidental

Likelihood: Moderate
Justification: This may accidentally occur often, as many technologies used here may utilize the ISM band.

Severity - Emergency Medical Service: High Availability Impact
Justification: The inability to relay information to the appropriate parties or call for help could lead to loss of life.

Severity - Fire Service: High Availability Impact
Justification: Firefighters being unable to communicate during an emergency fire situation could lead to loss of life of either the firefighter or the victim.

Severity - Law Enforcement: High Availability Impact
Justification: This could lead to loss of life if a police officer responds to a situation, is wounded, and is unable to call for help.

Source: Known Attacks – Jamming police Transmissions in Tampa, FL**;** Known Attacks – DDoS of Emergency 911 System

Mitigations:
Using wireless communication protocols that are more resistant to dumb and smart jamming attacks, such as frequency-hopping spread spectrum (FHSS). Certain protocols are more resistant to protocol jamming than others and should be carefully considered before implementation. Wired devices and earpieces may be useful but will ultimately need to connect to a wireless device that may be vulnerable to these types of attacks.

7.2.6 Structural or architectural issues interference

Threat Description: Structures or other environments that public safety personnel may venture into as part of their work may not allow cellular and other signals to properly penetrate.
Vulnerability: Radio frequencies lack sufficient signal strength to penetrate the environment, and public safety personnel operate in enclosed environments.

Threat Source: Failure of controls

Likelihood: High
Justification: Structures and surrounding environments are some of the most common causes of interference. The density of materials, such as concrete and steel, can weaken or block radio signals.

Severity - Emergency Medical Service: High Availability Impact
Justification: The inability to relay information to the appropriate parties or call for help could lead to loss of life.

Severity - Fire Service: High Availability Impact
Justification: Firefighters may go into a burning structure with or without solid communications in place. Being unable to communicate during an emergency fire situation could lead to loss of life of either the firefighter or the victim.

Severity - Law Enforcement: High Availability Impact
Justification: During an active shooter event, law enforcement must be able to relay critical information to fellow responders both inside and outside of the building. A lack of communications could result in additional causalities, loss of life, or other threats to public safety.

Source: Known Attacks – Washington, D.C. Navy Yard Radio Failure

Mitigations:
Mobile devices can use wireless frequencies that better penetrate walls and common building materials. Repeaters and other communication technology that allow information to be chained to an external source of connectivity can assist in providing a consistent line of communication. Research of indoor coverage is ongoing within the Mission Critical Voice (MCV) portfolio at PSCR [58]. This research may assist in resolving the structural threat to mobile devices.

7.2.7 Unreliable communications channel due to interoperability issues

Threat Description: Public safety jurisdictions utilize a specific set of channels for communications. In an emergency, neighboring jurisdictions may be called in to assist. The radios of different jurisdictions may not be configurable to use the same channels, and this could disrupt communication.

Vulnerability: Disparate technology configurations across jurisdictions may not be interoperable.

Threat Source: Failure of Controls
Likelihood: Moderate
Justification: While this threat does exist, jurisdictions typically designate a separate channel or a set of radios to distribute to outside public safety personnel at the scene of an incident.

Severity - Emergency Medical Service: Availability Moderate Impact
Justification: While alternate options for communication would allow EMS responders to perform tasks and communicate with their local jurisdiction, communication may still be limited.

Severity - Fire Service: Moderate Availability Impact
Justification: This could cause availability issues, especially with the user interface, if firefighters must switch to alternate communications channels that require a fair degree of configuration.

Severity - Law Enforcement: Moderate Availability Impact
Justification: Limitations to device channel configuration could cause communication issues, though law enforcement officers can still retain some instance of communication to actively respond to an emergency.

Source: Known Attacks – Antiquated and Inoperable Communication Systems

Mitigations:
Mobile devices can use interoperable communications equipment, protocols, and security technologies. In fact, the use of LTE technology mitigates several the interoperability issues traditionally associated with LMR. Having a pre-specified method for communications fallback may provide a means of communication if there is an incompatibility issue. A jurisdiction may need to allocate a supply of devices to distribute when external jurisdictions do not have interoperable devices.

7.2.8 Device failure due to a lack of ruggedization

Threat Description: A device not designed for resistance to harsh environments could fail, leaving the public safety official without a means of communication.

Vulnerability: Components of the mobile device may not be rated to handle extreme hot and cold temperatures, exposure, or submersion in liquid.

Threat Source: Environmental, Human error

Likelihood: Low
Justification: Public safety practitioners would likely try to use public safety-grade, ruggedized devices where possible.

Severity - Emergency Medical Service: High Availability Impact
Justification: Being unable to relay information to the appropriate parties or call for help could lead to a loss of life.
Severity - Fire Service: High Availability Impact
Justification: Firefighters' inability to communicate in an emergency fire situation could result in loss of life to either the firefighter or the victim.

Severity - Law Enforcement: High Availability Impact
Justification: This could lead to loss of life if a police officer responds to a situation, is wounded, and is unable to call for help.

Source: N/A

Mitigations:
The use of devices resistant to external sources of stress, such as temperature, liquid, or shock, can ensure reliability during an emergency. The International Protection Marking standard (IEC 60529), informally known as the Ingress Protection (IP) rating system, measures a smartphone's resistance to water, dust, and other particles and may be a useful when evaluating devices. Although this is a serious issue, it is included for awareness and is considered outside of the scope of PSCR's research activities.

7.2.9 Mobile device is infected with malware resulting in a loss of sensitive information

Threat Description: Public safety mobile devices could be attacked by mobile malware, which may store and relay public safety information to malicious entities.

Vulnerability: The device can be exposed to malicious users through a lack of OS and/or application updates, poor implementation of software assurance concepts by the developer, and inadequate application vetting tools and procedures for device apps.

Threat Source: Adversarial

Likelihood: Moderate
Justification: Although malware is common on mobile devices, developers often resolve malware issues and send patches or updates to the mobile devices or applications. Typically, a mobile device is not vulnerable to known malware for long.

Severity - Emergency Medical Service: Moderate Confidentiality Impact
Justification: This information could contain personal details about patients, such as first name, last name, address, insurance information, medical history, and current injuries, all of which is subject to HIPAA regulations. This would be unlikely to result in a loss of human life.

Severity - Fire Service: Low Confidentiality Impact
Justification: An adversary with access to this information would be unlikely to pose a threat to a firefighter's immediate survival of the emergency situation at hand.

Severity - Law Enforcement: High Confidentiality Impact
Justification: The classification of this data depends on the type of incident at hand. The high impact level is assigned because there exists the possibility of loss of life. For instance, sensitive information shared at a crime scene or an undercover officer simply communicating with law enforcement could lead to loss of life. It is of note that much of a law enforcement officer's routine communication is sent securely, making this classification situation-dependent.

Source: Known Attacks – Unauthorized Access at Fire Station

Mitigations:
Mobile management solutions may assist with automated patching or by notifying the user of security patches and updates that should be routinely monitored and implemented. Software and firmware developers, in particular, should give proper consideration to risks associated with the supply chain. Applications installed on public safety mobile devices and wearables should be properly vetted before installation and use. Mobile threat defense technology can also help identify certain applications as malware, and NIST SP 800-163 [45] can assist with the vetting of mobile applications.

7.2.10 Location tracking of a public safety mobile device

Threat Description: Mobile devices may inadvertently relay identifying information about itself through WiFi or LTE identifiers. Additionally, public safety devices may be purchased in bulk with a hardware address range that may be known by malicious actors. Finally, installed applications could programmatically access a device's location information.

Vulnerability: Many wireless protocols and devices regularly transmit unencrypted permanent identities that can be stored and tracked. Applications may access and retrieve a mobile device's location.

Threat Source: Adversarial

Likelihood: Moderate
Justification: COTS WiFi, Bluetooth, and LTE devices regularly expose this information. If a public safety device is being used in a BYOD scenario, it is much more likely that a malicious or dangerous application is installed.

Severity - Emergency Medical Service: Low Confidentiality Impact
Justification: Being able to track an EMT would not lead to loss of life or severely impact day-to-day operations.

Severity - Fire Service: Low Confidentiality Impact
Justification: Being able to track a firefighter would not lead to loss of life or severely impact day-to-day operations.

Severity - Law Enforcement: High Confidentiality Impact
Justification: If a malicious user could track an officer's device entering an area, they could evade their presence or place the officer in danger. If an undercover agent's device is targeted, it could reveal their identity and result in loss of life.

Source: N/A
Mitigations:
Randomized or obfuscated permanent identifiers can be leveraged by protocols and devices to obscure information about the mobile device's user or location. This could be accomplished using a whitelist of wireless network associations by default, followed by a move to a more typical advertisement system if devices from the whitelist are not found. Mobile Threat Defense is a product category that can help detect applications that maliciously obtain a user's location. Application vetting can help detect overzealous applications that might access this information.

7.2.11 Malicious management profile or certificate is installed on a device

Threat Description: Mobile devices can be sent special administrative requests that offer high levels of privilege on the device to a third party. These requests are known as enterprise mobility management (EMM) profiles or administrative profiles. The profiles offer some level of administrative access to the device and can provide an attacker visibility to a device user's identity and the type of device they have. Additionally, these profiles can be used to install malicious applications onto the device without going through the normal application vetting process offered by a mobile application store.

Vulnerability: First responders may unknowingly accept the profile when presented with it. Alternatively, they may choose to install free versions of paid applications.

Threat Source: Adversarial, Accidental

Likelihood: Moderate
Justification: A malicious profile or certificate may accidentally be installed by a user who is unaware of its validity and needs immediate access to data.

Severity - Emergency Medical Service: Moderate Confidentiality Impact
Justification: A malicious application could glean patient information that is subject to HIPAA regulations, including a patient's medical history. This would be unlikely to result in a loss of human life.

Severity - Fire Service: Low Confidentiality Impact
Justification: An adversary having access to a device or confidential information poses an unlikely threat to a firefighter's survival or well-being.

Severity - Law Enforcement: High Confidentiality Impact
Justification: If a malicious user could track an officer's device entering an area, they could evade their presence or place the officer in danger. If an undercover agent's device is targeted, it could reveal their identity and result in loss of life.

Source: N/A

Mitigations:
Appropriate training can enable users to identify legitimate enterprise mobility management profiles, though IT staff may wish to be the only party that can accept and install them. Mobile threat defense technology can also help identify known malicious MDM profiles. At the time of this writing, MDM profiles can generally only have one profile installed on a device at a time. Therefore, an agency or organization that is already using MDM profiles may already have a mitigation in place.

7.3 Threats to Public Safety Wearable Devices

The following threats pertain to the use of public safety wearable devices.

Table 6: Threats to Public Safety Wearable Devices

Threat Event	Vulnerability	Category	Source	Severity	Likelihood
Sensitive information is intercepted from a wearable device	Lack of confidentiality protection	Confidentiality	Adversarial	EMS: Mod Fire: Low LE: High	Low
Malicious user spoofs wearable device and sends false information	Lack of integrity protection and mutual authentication	Integrity	Adversarial	EMS: High Fire: High LE: Mod	Low
Malware on backend public safety infrastructure prevents wearable device from properly functioning	Unpatched Software	Availability	Adversarial	EMS: Mod Fire: High LE: Low	Low

Malicious attack on wearable device that causes battery drain, overheating, or explosion	Software weakness or unpatched software	Availability	Adversarial	EMS: Mod Fire: High LE: Low	Low
Location tracking of public safety wearables	Lack of temporary identities	Confidentiality	Adversarial	EMS: Low Fire: Low LE: High	Mod
A denial-of-service or other technical attack jams wearable communications	Protocol not designed to withstand jamming attacks; lack of available spectrum	Availability	Adversarial, Accidental	EMS: Mod Fire: High LE: Low	Mod
Application within wearable device is infected with malware, resulting in a loss of sensitive information	Lack of OS and/or application updates exposed device to malicious users	Confidentiality	Adversarial	EMS: Mod Fire: Low LE: High	Low

7.3.1 Sensitive information is intercepted from a wearable device

Threat Description: A malicious entity eavesdrops on public safety traffic during an emergency situation. This threat includes sniffing Bluetooth microphones and earpieces and using sensors to monitor medical information.

Vulnerability: Wearables tend to have weaker operating systems and insufficient patching mechanisms. This leaves wearables susceptible to several distinct vulnerabilities that could be exploited. The simplest vulnerability is a lack of encryption for the data path used by the mobile device, including cellular, WiFi, and Bluetooth. Additionally, broken cryptographic algorithms and insufficient key sizes could also be used to access plaintext content of communications.

Threat Source: Adversarial

Likelihood: Low
Justification: Adversaries would need to be close in proximity to the wearable devices.

Severity - Emergency Medical Service: Moderate Confidentiality Impact
Justification: A malicious application could glean patient information that is subject to HIPAA regulations, including a patient's medical history. This would be unlikely to result in a loss of human life.

Severity - Fire Service: Low Confidentiality Impact
Justification: An adversary having access to a device or confidential information poses an unlikely threat to a firefighter's survival or well-being.

Severity - Law Enforcement: High Confidentiality Impact
Justification: If a malicious user could track an officer's device entering an area, they could evade their presence or place the officer in danger. If an undercover agent's device is targeted, it could reveal their identity and result in loss of life.

Source: Use Case – Wearable Integrated Sensor Technology; Use Case – Bodycam; Use Case – Patient Monitor

Mitigations:
Cryptography can be used to provide confidentiality protection for public safety communications. If the wearable devices have a cellular radio, encryption can be implemented by the network, which simplifies algorithm selection and cryptographic key management issues. Unlike mobile devices, current wearable devices rarely have cellular radios. This may restrict the type of algorithms and length of key sizes. For more complicated wearables, encryption could also be provided by a third-party application, but this is not commonly available.

7.3.2 Malicious user spoofs wearable device and sends false information

Threat Description: An individual may be able to send false sensor information or other data that may be trusted by a mobile device.
Vulnerability: A lack of integrity protection or mutual authentication protocols can lead to compromised data.

Threat Source: Adversarial

Likelihood: Low
Justification: This type of incident has not been recorded in the past.

Severity - Emergency Medical Service: High Integrity Impact
Justification: If a sensor or other medical information is spoofed, an injured person could die. For instance, if the sensor says that a patient’s heart is functioning properly when their heart is experiencing problems, the patient may not receive necessary treatment.

Severity - Fire Service: High Integrity Impact
Justification: Spoofed sensor readings could lead a firefighter into an area of a burning structure that is much hotter than they initially believed, which could result in death.

Severity - Law Enforcement: Moderate Integrity Impact
Justification: A malicious user could send a falsified message about an active shooting to law enforcement, resulting in an unnecessarily heightened response that might potentially endanger the officers or the public.

Source: Use Case – Bodycam

Mitigations:
Integrity protection or digital signatures could authenticate data sources. However, such

capabilities are not easily available on all wearable devices. If wearables are wirelessly connected to a larger wireless network, restricting network access would also be beneficial.

7.3.3 Malware on backend public safety infrastructure prevents wearable device from properly functioning

Threat Description: Malicious software corrupts or disables backend infrastructure that is providing service to wearable devices. The wearable device is not able to function without connectivity to the service.

Vulnerability: Unpatched software or other software vulnerability can impede proper functioning of a wearable device.

Threat Source: Adversarial

Likelihood: Low
Justification: Although attacks on backend public safety infrastructure have been documented, these attacks have not necessarily impacted the use of wearables or other communications equipment.

Severity - Emergency Medical Service: Moderate Availability Impact
Justification: An EMS technician may place monitoring sensors on a patient and attempt to relay medical concerns to the destination hospital. If communications fail, physicians may not be prepared to treat incoming victims.

Severity - Fire Service: High Availability Impact
Justification: Wearable sensors may be unable to relay the fact that a firefighter is in need of immediate assistance.

Severity - Law Enforcement: Low Availability Impact
Justification: Police body cameras could cease to function due to streaming service issues. Evidence that would be useful in court may not be collected.

Source: Known Attacks – Ransomware Infecting Washington, D.C. Police Surveillance Equipment

Mitigations:
Hardware manufacturers and firmware developers should give proper considerations to risks associated with the supply chain. Malware detection systems can also be deployed onto the system. Many behavioral analysis systems establish a baseline of activity before they can detect malicious activity. If malware is included as part of that baseline, it may not be noticed.

7.3.4 Malicious attack on wearable that causes battery drain, overheating, or explosion

Threat Description: An attack on a wearable device could drain its battery, overheat the device, or cause the device to explode.

Vulnerability: Unpatched software may have known exploitable vulnerabilities.

Threat Source: Adversarial

Likelihood: Low
Justification: This type of incident has not been recorded in the past.

Severity - Emergency Medical Service: Moderate Availability Impact
Justification: Vital monitoring devices may cease to operate. EMS staff would not receive patient information in a timely manner, especially during a mass casualty event with multiple victims requiring attention. EMTs could resort to communicating with traditional mobile devices and medical equipment.

Severity - Fire Service: High Availability Impact
Justification: Firefighters are dependent on their wearables in emergency situations. Since the wearables are generally embedded underneath their personal protective equipment (PPE), the failure of a throat mic or earpiece could prevent firefighters from communicating that they require immediate assistance, which could result in death.

Severity - Law Enforcement: Low Availability Impact
Justification: Even if there is an issue with an officer's wearable device, they are still able to communicate through other means, such as a mobile device. The wearable device does not hinder the officer's ability to perform. Law enforcement officers would be able to compensate by switching to another form of communication, such as their mobile device.

Source: N/A

Mitigations:
The purchasing jurisdiction can research the wearable device’s software update policy as well as whether or not the manufacturer actually adhered to that policy in the past, as this does not always occur. Installing software updates is key to reducing exploitable vulnerabilities that can lead to these types of failures. If the wearable device is not updatable at all, it may not be recommended for use by public safety personnel.

7.3.5 Location tracking of public safety wearables

Threat Description: Wearables may beacon out identifying information about the device, such as WiFi or LTE identifiers. From another perspective, installed applications could programmatically access a device’s location information.

Vulnerability: A lack of temporary identities means that many wireless protocols and devices regularly transmit unencrypted permanent identities that can be stored and tracked.

Threat Source: Adversarial

Likelihood: Moderate
Justification: COTS WiFi, Bluetooth, and LTE devices regularly expose this information.

Severity - Emergency Medical Service: Low Confidentiality Impact
Justification: Being able to track an EMT would not lead to loss of life or severely impact day-to-day operations.

Severity - Fire Service: Low Confidentiality Impact
Justification: Being able to track a firefighter would not lead to loss of life or severely impact day-to-day operations.

Severity - Law Enforcement: High Confidentiality Impact
Justification: If a malicious user could track an officer's device entering an area, they could evade their presence or place the officer in danger. If an undercover agent's device is targeted, it could reveal their identity and result in loss of life.

Source: N/A

Mitigations:
Randomized or obfuscated permanent identifiers can be leveraged by protocols and devices to obscure wearable information (e.g., a whitelist of wireless network associations by default followed by a move to a more typical advertisement system if devices from the whitelist are not found).

7.3.6 A denial of service or other technical attack jams communications

Threat Description: A variety of technical DoS attacks exist, from exploiting protocol-specific vulnerabilities (e.g., WiFi disassociation frames) to smart jamming attacks and less sophisticated spectrum-jamming attacks. All of these can occur for any wireless protocol, including Bluetooth, WiFi, and LTE.

Vulnerability: The protocols used may not be designed to withstand jamming attacks or the lack of an available spectrum. Many deployed technologies will utilize the already noisy ISM band.

Threat Source: Adversarial, Accidental

Likelihood: Moderate
Justification: This may accidentally occur often as many public safety technologies utilize the ISM band. Numerous instances have been identified of jamming attacks from adversarial threat sources.

Severity - Emergency Medical Service: High Confidentiality Impact
Justification: Being unable to relay information to the appropriate parties or call for help could lead to loss of life.

Severity - Fire Service: High Confidentiality Impact
Justification: Firefighters being unable to communicate during an emergency fire situation could lead to loss of life of either the firefighter or the victim.

Severity - Law Enforcement: High Confidentiality Impact
Justification: If a police officer responds to a situation, is wounded, and is unable to call for help, this could lead to loss of life.

Source: N/A

Mitigations:
Public safety personnel can use wireless communication protocols that are more resistant to dumb and smart jamming attacks, such as FHSS. Certain protocols are more resistant to protocol-jamming than others and should be carefully considered before use. Wired devices and earpieces will ultimately need to connect to a mobile device that is vulnerable to these types of attacks, as documented in the previous section (7.2.5).

7.3.7 Application within wearable device is infected with malware resulting in a loss of sensitive information

Threat Description: Public safety wearable devices could be attacked by mobile malware, which may store and relay public safety information to malicious entities. Although not all wearable devices support "apps" in a manner similar to mobile devices, some more sophisticated wearables do.

Vulnerability: Lack of OS and/or application updates may expose a device to malicious users. Additionally, poor implementation of software assurance concepts by the developer and application vetting tools and procedures applied to apps may compromise a device.

Threat Source: Adversarial

Likelihood: Low
Justification: Malware designed to execute and steal information on a wearable platform is not yet commonplace, although this may change.

Severity - Emergency Medical Service: Moderate Confidentiality Impact
Justification: This information could contain personal details about patients, such as first name, last name, address, and insurance information. Additionally, information about a patient's medical history and/or current injuries could be exposed, all of which is data subject to HIPAA regulations. This would be unlikely to result in a loss of human life.

Severity - Fire Service: Low Confidentiality Impact
Justification: An adversary having access to this information would be unlikely to be a threat to a firefighter's immediate survival of the emergency situation at hand.

Severity - Law Enforcement: High Confidentiality Impact
Justification: This classification of this data depends on the immediate type of incident at hand. The high impact level is used since there exists the possibility of loss of life. For instance, sensitive information shared at a crime scene or an undercover officer communicating with law enforcement could lead to loss of life. It is of note that much of a law enforcement officer's traffic is routinely sent in in the clear, making this extremely situation-dependent.

Source: N/A

Mitigations:
Proper consideration should be given to risks associated with the supply chain, especially software and firmware developers. Applications installed on public safety mobile and wearable devices should be properly vetted before installation and use. Vetting applications on IoT and wearable applications are still in infancy, and guidance may not be readily available.

7.4 Areas Warranting Further Scrutiny

Following the threat analysis, two cited security problems are particularly worrisome. Each of these issues affects both mobile devices and wearables. These two issues warrant additional scrutiny and research and are detailed below.

7.4.1 Device and User Tracking

It is common knowledge that the physical location of wireless devices can be tracked. These devices are often physically placed in a user's jacket or pocket, and if the presence of the wireless device is known, the location and identity of the user may also be known. Tracking of users and their wireless devices can be a staging point for physical and digital attacks against specific public safety individuals. Wireless device tracking is possible in part because wireless devices must associate with an unknown host or controller. In the first step of this association process, a device announces ("advertises" or "beacons") its presence to other devices. These beacons may contain a permanent identifier, which could be used as an easily accessible tracking mechanism.

In the case of a cellular device, the International Mobile Subscriber Identity (IMSI) would be the advertised identifier. The SA3 working group may address this advertised identifier in future deployments of 5G [47]. For the 802.11 set of WiFi protocols, the identifier would be a media access control (MAC) address. As a final example, the Bluetooth identifier would be a Bluetooth MAC address, which is generated in a different manner than a typical MAC. WiFi and cellular permanent identities are typically unique across the entire world. Bluetooth permanent identities may be unique but are often simply the WiFi MAC address of a mobile device incremented by one digit.

The use of these permanent identifiers by public safety devices and wearables means that they can be tracked. This may not be relevant to some public safety disciplines (e.g., fire service, EMS), but members of law enforcement may face a different scenario. At times, the identity of a police officer needs to be a secret. It would be simple for malicious individuals to collect cellular, WiFi, and Bluetooth traffic outside of a police station for an extended period. This could be done by simply hiding an inexpensive microcomputer coupled with a power source near a police station. The device could collect these advertised identifiers for hours or days and be retrieved later once its power source is depleted. A law enforcement official simply walking near a hidden device located at a station's entrance could be enough to have their personal and public safety device IDs stored in a database. These databases could be combined with other similar databases and sold on illegal marketplaces.

With a database of law enforcement officials' unique device identifiers on hand, malicious individuals would have the ability to check any IMSI or MAC address they are currently receiving against a database in real time. They would then know if any law enforcement officials are in the vicinity. Law enforcement officials operating in an undercover capacity may be revealed, and personnel could be tracked to their personal residences.

However, technology exists to thwart this type of tracking, specifically the use of temporary and/or randomized identifiers such as 3GPP SA3 standardized Temporary Mobile Subscriber Identities (TMSIs) and GUTI (Globally Unique Temporary Identifiers), though these are not mandatory. WiFi and Bluetooth MAC randomization is also an option, but this may be implemented in non-standardized manner if at all. Encryption of the communications channel would not generally solve this issue as these identifiers are often unencrypted during the initial attach or pairing procedure. Additionally, wireless advertisements and beacons are generally not encrypted as these messages are intentionally broadcast for any user to view.

7.4.2 Attacks on Availability

Jamming continues to be an open, unresolved problem for the availability of wireless systems. This type of attack affects certain public safety disciplines more than others, specifically the fire service. A firefighter's life depends on constant access to voice communication services, so much so that it is a common practice for firefighters to use some version of the "buddy system" when entering a dangerous situation.

In the context of this document, we consider three types of jamming: wideband spectrum jamming (i.e., dumb jamming), narrowband spectrum jamming (i.e., smart jamming) and protocol jamming. Wideband jamming affects a large swath of the electromagnetic spectrum, likely multiple bands at once. Narrowband jamming affects only a small portion of the spectrum, anywhere from the ISM band to an individual carrier frequency that could be used to send a specific message. Protocol jamming is a nebulous term used to describe availability attacks against specific protocols and often removes a specific device's network access. One could make a reasonable argument that the use of the word "jamming" in this context is incorrect.

APCO P.25 has been and currently is susceptible to wideband and narrowband jamming attacks, as are most wireless systems. Protocol jamming attacks are not widely available or known for this closed wireless system. LMR uses protocols and devices that have generally avoided the type of scrutiny offered to commercial devices and protocols by the cybersecurity community. With the introduction of modern mobile devices, this is no longer the case. The wireless protocols used by modern mobile devices are also susceptible to these smart and dumb jamming attacks. Yet protocol jamming attacks are well-documented, simple attacks that require inexpensive hardware and little expertise. The following table shows how this is an increase in attack surface.

Table 7: Summary of Jamming Attacks on Device Types

	LMR Devices	Public Safety Smartphones
Wideband	✓	✓
Narrowband	✓	✓
Protocol	X	✓

WiFi allows any nearby user to remove any other user from a WLAN. This is possible via deauthentication frames, which then require a user's device to authenticate to the network again. WiFi also allows for a similar disassociation frame to be sent that completely removes an established connection between an access point (AP) and client. These "protocol jamming" methods are built into the standard as a feature. LTE suffers from a similar issue as REJECT messages can be sent to devices during the LTE radio association process which, depending on implementation, could put a device into airplane mode without informing the user. Any of these messages can be sent by anyone as there is no security applied to them, such as authentication or integrity protection.

The availability impact on wearables differs across the three disciplines. In general, law enforcement operations allow for officers to fall back on mobile devices when a wearable device fails. EMS relies on wearable devices to inform them of patient health and vitals where the data is critical for triaging and treating patients, especially during a mass casualty incident. Fire fighters have the greatest dependency on wearables for communicating during an incident. Their wearable and other communication equipment must be embedded within their fire suits. If a device fails, fire fighters may be limited in communication abilities until they can relocate to a safe area, which can result in life-threatening situations. Therefore, it may be prudent for firefighters to only use wearables that are resistant to easily performed protocol jamming attacks. Introducing these types of technology creates an entirely new attack surface that public safety is unaccustomed to dealing with, unlike wideband and narrowband jamming which will remain an unaddressed threat and is generally considered acceptable. It may be prudent to encourage the use of wireless protocols that are immune to these types of attacks for critical voice communication.

8 Security Objectives

Security objectives were identified based on the analysis of interview information and the threats existing within the defined threat model. Some objectives have associated sub-objectives that are further elaborated upon. Each objective is introduced and mapped to any associated threats. The following principles are presented and discussed in no particular order.

- Availability
- Ease of Management
- Interoperability
- Isolation
- Confidentiality
- Authentication
- Integrity
- Healthy Ecosystem

8.1 Availability

Availability refers to "ensuring timely and reliable access to and use of information" [10]. This characteristic was the primary objective communicated from the interviewed public safety personnel. Availability is a multifaceted concept and exists in a variety of forms, such as network availability, network agility, data availability, and device availability. These sub-objectives are discussed below.

8.1.1 Network Availability

Public safety personnel require constant access to voice and data networks to perform their duties. Supporting networks must be able to handle high traffic during an incident without failing. On an occasion when a network fails, failure needs to occur in a graceful manner. A graceful shutdown may include notifying public safety professionals, so they can switch to some other means of communication. Mobile devices may attempt to switch to a different wireless communication technology, such as point-to-point LTE, WiFi, or possibly satellite networks. Wearables are likely to be part of a PAN that often utilize wireless technologies that operate only within limited distances. Bluetooth (IEEE 802.15) and WiFi (IEEE 802.11) are prime examples but not the only possibilities. Wearable devices may also contain a cellular modem capable of communicating over LTE.

8.1.2 Network Agility

Network agility refers to the ability to switch between available networks should one communication method fail. This aspect of availability includes the ability to modulate to other channels and frequencies and use other wireless technologies. For instance, if an LTE public safety network fails, a law enforcement officer would be able to switch to a different LTE network. If a wearable device acting as part of a Bluetooth PAN is jammed due to electromagnetic interference, the wearable may attempt to connect to WiFi and subsequently try activating an LTE radio.

8.1.3 Data Availability

This aspect of availability ensures that public safety data can acquire access when needed. For instance, bone conduction technology is a useful capability as it allows firefighters to hear voice traffic inside of a fire, which is extremely loud. This same principle can be applied to throat mics for firefighters. Data availability would also be disrupted if a public safety mobile device was attacked via ransomware. A public safety employee being unable to access data due to ransomware would violate data availability.

8.1.4 Device Availability

Public safety devices must operate in harsh environments. This includes extremely hot and cold temperatures, liquid submersion, and electromagnetic interference. Devices must also be able to survive drops and withstand heavy weight while remaining operational. The level of required device availability or ruggedness is unclear at this time because there is no unified public safety standard, although several military and industry standards exist.

Different public safety original equipment manufacturers (OEMs) may ship devices with different Ingress Protection (IP) ratings or resistance to shock absorption. Other device ruggedization standards exist but public safety may need to define their own standard that meets their durability needs. If possible, the device should notify public safety device owners before a device reaches its ruggedized design limitations (e.g., maximum impact or high temperature limit). This should provide ample time to switch to another communications method or at least inform others of the failure before it occurs.

8.2 Ease of Management

Certain conditions could require immediate updates to devices in a PAN. Currently, LMR keying and channel settings can require a radio to be taken out of commission, plugged into another system, updated, and then put back into commission. This process is not conducive to public safety's immediate response needs during an emergency. Ease of management should provide a secure, reliable, and efficient way to deploy and maintain devices within an organization. To achieve this, a radio operations group should have systems and devices that support over-the-air rekeying, multiple encryption keys, and system updates.

Configuration management allows cellular and radio operators to set key parameters on a device. For cellular devices, a mobility device management (MDM) solution enables an administrator to configure settings such as device timeout, pin/password, approved applications, and email.

8.3 Interoperability

Public safety communications systems are currently dependent on LMRs, so mobile devices and wearables must be interoperable with LMR. According to NIST SP 1108, interoperability is defined as "the capability of two or more networks, systems, devices, applications, or components to exchange and readily use information—securely, effectively, and with little or no inconvenience to the user."[48] Interoperability will be necessary for various aspects of public safety's communication spectrum. These different aspects of interoperability are described below.

8.3.1 Device Configuration Interoperability

Device configuration interoperability ensures that devices that function within one public safety jurisdiction can function in a similar manner within another. This assumes that the device has the correct credentials to communicate between different jurisdictions and may require key provisioning to access a different communication interface.

8.3.2 Infrastructure Interoperability

With new devices being developed every day, it would be beneficial if the devices easily integrated into the current public safety infrastructure. Interoperability between different devices and systems is important to reduce costs and allow easy integration into the public safety's system infrastructure.

8.3.3 Network Interoperability

Given the potential for multiple distinct but concurrently functioning cellular public safety networks, it is important that devices function the same regardless of what network they are using. Lack of interoperability between the networks may restrict communication capabilities and thus reduce situational awareness at an emergency incident.

8.3.4 Device Platform/Application/Services Interoperability

LMRs, cellular devices, and wearables are built on different platforms and operating systems. Regardless of the baseline platform of the device, the communication between the devices should be seamless to allow the first responders to focus on the emergency incidents. Applications and services developed to aide first responders should be available for use on all device platforms.

8.3.5 Security Technology Interoperability

This type of interoperability stems from the need to have security technologies capable of exchanging security information such as cryptographic keys. Current practices for exchanging security information differ somewhat from jurisdiction to jurisdiction. Desktop applications are sometimes needed to properly provision LMR devices, and when multiple jurisdictions are responding to the same incident, each jurisdiction's management application may need to be used. These applications can be expensive and difficult to manage. Alternatively, some jurisdictions support OTAR, whereas others do not. With security technology interoperability, security-relevant information can be easily exported, digested, and exchanged.

8.3.6 Data Format Interoperability

When sharing data, public safety-specific information should be provided in a common public format understandable by all systems and personnel. The information exchanged between different systems should be capable of receipt and interpretation.

8.4 Isolation

Isolation is the ability to keep data components and processes separate from one another. In particular, it is the ability to restrict the flow of information from one entity to another. Modern mobile devices provide varying levels of isolation, and this capability may not be present at all in many wearables.

8.4.1 Data Isolation

Multiple public safety personnel stated that personal and public safety information needed to be kept separate. One common way of doing this on a mobile device is through the use of a "secure container." Wearables often lack the ability to separate data, but wearables are often single-purpose, dedicated, embedded devices that do not contain data from multiple services, although this may change in the future.

8.4.2 Application Isolation

Application isolation keeps one application from interacting with another unless it is an intended interaction. This helps keep devices running in a secure state and can prevent application exploits from being successful or at least limit their impact.

8.5 Confidentiality

Confidentiality means "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information" [10]. Confidentiality protection often occurs via access controls and data encryption. Encryption of public safety data, both in transit and at rest, did not have the same priority for every public safety discipline. For example, members of the fire service consistently identified the need for availability over data confidentiality. Law enforcement and the EMS needed data confidentiality under certain scenarios.

Interviews with public safety professionals showed that encrypted connections are not used in every public safety discipline. While confidentiality protection may provide security benefits, it also contains drawbacks. Setting up secure connections may be a complex technical process with significant network bandwidth, usability, and interoperability barriers. This supports the "ease of management" objective.

8.5.1 Data in Transit

Data in transit refers to protecting data transmitted over a network connection, such as protecting a patient's information as it is transmitted from an EMT's radio to a hospital. Another example is ensuring that a Bluetooth throat microphone is securely communicating with a mobile device.

8.5.2 Data at Rest

Data at rest refers to protecting data stored on a device, such as encrypting pictures of a crime scene taken by a police officer or patient data encrypted on a mobile device during transport in an ambulance.

8.6 Authentication

NISTIR 7298, *Glossary of Key Information Security Terms* defines authentication as "verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system" [10]. Authentication is necessary to ensure that only authorized public safety users have access to public safety resources. Below are types of authentications that are applicable to public safety.

8.6.1 Ease of Authentication

First responders need to have an efficient way of authenticating to their device(s) in emergency situations. Complicated passwords and authentication tokens can interfere with the first responder's focus on the mission. Multiple authentication methods exist and should be analyzed for use. NISTIR 8080 *Usability and Security Considerations for Public Safety Mobile Authentication* discusses this and other usability issues first responders face as well as how they impact other areas of security [11].

8.6.2 User to Device Authentication

In many instances, especially law enforcement, it is important to prevent external entities from accessing information stored on a lost or stolen device. User to device authentication does not prevent sensitive information from appearing on the lockscreen via notifications. Notifications to a locked device are available to anyone who has physical access to the device.

8.6.3 Device to Network Authentication

During large-scale emergency events, telecommunication networks tend to become extremely congested. Priority and preemption for public safety users is necessary to ensure that they can communicate with each other, and proper authentication ensures successful implementation. In addition, there is the simple requirement of ensuring that unauthorized devices are not allowed to access the network.

8.6.4 User to Third-party Service, Wearable, or Device Authentication

Users may also need to authenticate to individual applications, wearables, and third-party services. This authentication provides another layer of security to a first responder's device and applications. If a device is compromised, an unauthorized user would not be able to access public safety information on applications or devices due to strong authentication requirements.

8.7 Integrity

Integrity guards against improper data modification or destruction and includes ensuring information non-repudiation and authenticity [10]. Mobile devices must protect against corruption in hardware, firmware, and software. A rooted or "jailbroken" device bypasses system integrity checks, allowing the underlying OS and firmware to be manipulated—possibly unbeknownst to the user. This poses a significant risk to data and voice communications and applications used to access agency assets. Device manufactures can strengthen their validation methods by deploying a hardware root of trust (e.g., secure enclave, secure element).

Device manufacturers can customize the low-level OS and boot functions through a boot ROM agent that validates the boot loader and OS. This boot ROM agent acts as an additional root of trust and is critical to ensuring the operating system and firmware have not been tampered with.

8.8 Device and Ecosystem Health

8.8.1 Configurations

Public safety mobile devices may be customized for first responder's operational needs. Customized device operating systems can significantly vary in versions that ship with standard commercial devices. Large portions of the OS may be missing, modified, or replaced. Public safety device OEMs may also add new features unique to public safety to the OS, which may not receive the same level of security assessment as when implemented on large-scale deployment commercial devices. Due in part to these changes to the mobile OS, default security configurations and settings may not be configured in the same way as traditional COTS devices. This includes device encryption, pre-installed applications, authentication options, and other configuration options. While these configurations may assist in deployment to the field and be useful to public safety, minor misconfigurations can greatly affect the overall security of the device.

8.8.2 Updates

Over time, software, firmware, and hardware vulnerabilities are commonly identified in any information system. These issues may be exploitable by an adversarial threat source, leaving public safety devices vulnerable to many forms of security exploits. Closing these holes is most often performed by software updates and the security patching process. Yet many distinct organizations work in concert to supply the hardware and software components of smartphones and wearables, making the update process cumbersome. For instance, any device with a cellular radio has additional parties in this supply chain such as cellular carriers and baseband chipset designers.

It is difficult for many distinct entities to work together to develop, test, and deploy patches to such diverse systems, and it is challenging to coordinate between those entities to provide timely and effective updates that do not disrupt the functionality of the device. As such, a patch for the operating system could take a few months to over a year to reach the end-users' device. A device hardware manufacturer may also opt to delay updates in order to preserve the stability of device and application functionality. Users may need to weigh the risk of delayed security patches against device stability for their operations.

8.8.3 Bundled Applications

As previously mentioned, first responder applications are often preinstalled on public safety mobile devices. These applications provide functionality like PTT, computer aided dispatch (CAD) alerts, and local event notifications. Mobile applications receive some security review through the third-party application store (e.g., Apple App Store, Google Play, and the new FirstNet App Developer Program) before they are posted. A device manufacturer can also install applications onto a device through their own app store or by side-loading (i.e., manually installing). Regardless of installation origin, these applications should be vetted, monitored, and updated in a timely manner.

9 Conclusions

This study performed foundational research at the intersection of cybersecurity and public safety communications, and it helps to form the foundation for how to ensure the security and reliability of public safety communications. Relevant public safety use cases for mobile devices and wearables were identified, and the cybersecurity considerations for use cases were analyzed. Previous attacks on public safety systems were described, informing a threat analysis to analyze how potential security issues may affect public safety agencies. Finally, the information gleaned from this study was used in conjunction with information collected directly from interviews with public safety professionals to define security objectives for mobile devices and wearables.

Public safety has an inherent need for availability of telecommunications systems whereas confidentiality and integrity are sometimes considered secondary and tertiary needs. The results of this study support the notion that mobile devices, tablets, and wearables used by public safety have a very strong need for availability. Yet a more nuanced view is necessary, as confidentiality and integrity must also be thoroughly evaluated within each public safety discipline. For instance, the fire service requires high availability, whereas law enforcement and the EMS have regulatory considerations for data confidentiality (e.g., HIPAA). Depending on the emergency situation, the fire service may also require data confidentiality if the firefighter is handling patient information. That said, the type of emergency incident also contributes to the evaluation of the necessary security objectives for each public safety discipline.

A major conclusion of this effort is the need to develop robust and innovative mitigations for the threats identified within this report, along with practical guidance for their implementation. The transition from LMR to cellular technologies will take time but will also introduce a plethora of new technologies. Technologies like EMM to manage devices, mobile threat defense for endpoint protection, application vetting to ensure apps are safe and free of vulnerabilities, and encryption to prevent eavesdropping are all necessary to protect public safety communications. All of these are sufficiently complex, requiring an experienced professional to implement and properly configure them.

Little guidance exists for the appropriate configurations for public safety devices, let alone configurations for specific disciplines. These new technologies have a strong potential to introduce new vulnerabilities into a jurisdiction’s network. Therefore, it is important for this class of devices to be scrutinized in a manner similar to COTS devices or perhaps even more so given the sensitivity of public safety data. Yet to date, there are few examples of such a security analysis from academic, government, or industry security professionals.

Under PSCR’s security portfolio, there is authentication research with regards to mobile single sign-on (SSO) [59]. This research analyzes how mobile SSO can be implemented on a mobile device and used by first responders to authenticate once and gain access to multiple services on their devices. This research analyzes ease of authentication requirements, improving authentication assurance, and federating identities and user account management.

Within PSCR’s mission critical voice (MCV) portfolio, there is research into the availability concerns for first responders. The research considers in-building communication coverage.

More specifically, the research identifies ways to assess the in-building measurement and coverage quality of LTE. This research will provide first responders with awareness of LTE coverage within assessed buildings and ultimately improve coverage in such areas.

It is critical that the transition of public safety communications systems and devices to next generation technology occur in a smooth manner. By understanding the threats and risks posed to public safety systems and their users, life-threatening scenarios can be prevented from escalating due to malicious or accidental failures of technology. The following topics are open research areas in this space:

- Prevention of public safety device and user tracking
- Discipline-specific EMM policy configurations
- Low cost ways to implement EMM and mobile supporting technology
- Mitigations for protocol-jamming attacks that do not require redesigns of public safety devices
- Methods to add confidentiality and integrity protection to low cost wearables that insecurely transmit public safety information
- Best practices for updating the software on mobile devices and wearables
- Device lockscreen timeout recommendations
- Authentication mechanisms that have high assurance but are simple and non-intrusive
- Operational guidance for device sharing
- Ruggedizing mobile devices and wearables to public safety needs

For more information on this and other NIST security and public safety communications projects, please visit https://www.nist.gov/ctl/pscr/newsroom.

Appendix A—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

2G	2nd Generation
3G	3rd Generation
3GPP	3rd Generation Partnership Project
4G	4th Generation
5G	5th Generation
APCO	Association of Public Safety Communications Officials
BYOD	Bring Your Own Device
CAD	Computer-aided Dispatch
CERT	Computer Emergency Response Team
CISA	Cybersecurity and Infrastructure Security Agency
COTS	Commercial Off-The-Shelf
DC	District of Columbia
DHS	Department of Homeland Security
EMM	Enterprise Mobility Management
EMS	Emergency Medical Services
EMT	Emergency Medical Technician
EPCR	Electronic Patient Care Reporting
FHSS	Frequency Hopping Spread Spectrum
FM	Frequency Modulation
GhZ	Gigahertz
GPS	Global Positioning System
GSM	Global System for Mobile Communications
IEEE	Institute of Electrical and Electronics Engineers
IR	Interagency Report
IoT	Internet of Things
ISM	Industrial, scientific and medical
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
KBA	Knowledge-based authentication
LE	Low Energy
LEO	Law Enforcement Officer
LMR	Land Mobile Radio
LTE	Long Term Evolution
MCI	Mass Casualty Incident
MCV	Mission Critical Voice
MDT	Mobile Data Terminal
MFA	Multifactor Authentication
MHz	Megahertz
NCIC	National Crime Information Center
NFC	Near Field Communication
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology

NPSBN	Nationwide Public Safety Broadband Network
NPSTC	National Public Safety Telecommunications Council
OS	Operating System
OTP	One-Time Password
P25	Project 25
PAN	Personal Area Network
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PPE	Personal Protective Equipment
PSAC	Public Safety Advisory Committee
PSCR	Public Safety Communications Research
PTT	Push-To-Talk
RFID	Radio-Frequency Identification
SCBA	Self-Contained Breathing Apparatus
SIM	Subscriber Identity Module
SME	Subject Matter Expert
SoR	Statement of Requirements
SP	Special Publication
SSO	Single Sign-on
TLS	Transport Layer Security
UI	User Interface
UICC	Universal Integrated Circuit Card
UHF	Ultra High Frequency
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
VDI	Virtual Desktop Infrastructure
VHF	Very High Frequency
VPN	Virtual Private Network

Appendix B—References

[1] Middle Class Tax Relief and Job Creation Act of 2012, *PUBLIC LAW 112–96*, February 22, 2012. http://www.gpo.gov/fdsys/pkg/PLAW-112publ96/pdf/PLAW-112publ96.pdf [accessed 11/19/17].

[2] Ogata, Michael, *NISTIR 8135 - Identifying and Categorizing Data Types for Public Safety Mobile Applications: Workshop Report*, National Institute of Standards and Technology, May 2016. https://doi.org/10.6028/NIST.IR.8135.

[3] 3rd Generation Partnership Project, Service requirements for the Evolved Packet System (EPS), 3GPP TS 22.278 V13.2, 2014. http://www.3gpp.org/DynaReport/22278.htm [accessed 11/19/17].

[4] M. Souppaya and K. Scarfone, *Guidelines for Managing the Security of Mobile Devices in the Enterprise,* NIST Special Publication (SP) 800-124 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, June 2013, 29pp. https://doi.org/10.6028/NIST.SP.800-124r1.

[5] Brown et. al, Asessing Threats to Mobile Devices & Infrastructure: The Mobile Threat Catalogue, National Institute of Standards and Technology, September 2016. https://csrc.nist.gov/CSRC/media/Publications/nistir/8144/draft/documents/nistir8144_draft.pdf [accessed 11/19/17].

[6] NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013 (including updates as of January 15, 2014), 460pp. https://doi.org/10.6028/NIST.SP.800-53r4.

[7] Johnson, Ryabn, Kryptowire Discovered Mobile Phone Firmwqare that Transmitted Personally Identifiable Information Without User Consent or Disclosure, Blackhat 2016. https://www.blackhat.com/docs/us-17/wednesday/us-17-Johnson-All-Your-SMS-&-Contacts-Belong-To-Adups-&-Others-wp.pdf [accessed 11/19/17].

[8] Padgette et al, *Special Publication (SP) 800-121 Rev 2: Guide to Bluetooth Security,* National Institute of Standards and Technology, May 2017. https://doi.org/10.6028/NIST.SP.800-121r2.

[9] Bartock, Cichonski, Franklin, *Guide to LTE Security*, NIST Special Publication (SP) 800-187, National Insitute of Standards and Technology, November 2016. https://doi.org/10.6028/NIST.SP.800-187.

[10] National Institute of Standards and Technology, *NISTIR 7298 Revision 2 - Glossary of Key Information Security Terms*, May 2013. https://doi.org/10.6028/NIST.IR.7298r2.

[11] Choong, Greene, Franklin, *NISTIR 8080 - Usability and Security Considerations for Public Safety Mobile Authentication*, National Institute of Standards and Technology, July 2016. https://doi.org/10.6028/NIST.IR.8080.

[12] National Institute of Standards and Technology, *Special Publication (SP) 800-30, Guide for Conducting Risk Assessments Rev 1*, September 2012. https://doi.org/10.6028/NIST.SP.800-30r1.

[13] National Institute of Standards and Technology, *Special Publication (SP) 800-63-3, Electronic Authentication Guideline*, 2017 (includes updates as of 12-01-2017). https://doi.org/10.6028/NIST.SP.800-63-3.

[14] Public Safety Advisory Committee, Use Cases for Interfaces, Applications, and Capabilities for the Nationwide Public Safety Broadband Network, July 21, 2014. http://www.firstnet.gov/sites/default/files/PSAC Use Cases Report.pdf [accessed 11/19/17].

[15] National Public Safety Telecommunications Council, Priority and Quality of Service in the Nationwide Public Safety Broadband Network, Priority and QoS Working Group, Revision 1.4, August 2015. http://www.npstc.org/download.jsp?tableId=37&column=217&id=3515&file=PQoS15_003_PQoS_Definition_v1_4_20150817_GB_APPROVED.pdf [accessed 11/19/17].

[16] SAFECOM, Statements of Requirements for Public Safety Wireless Communications & Interoperability, Department of Homeland Security, Version 1.1, January 26, 2006. http://www.npstc.org/documents/SRSoR_V11_030606.pdf [accessed 11/19/17].

[17] FirstNet, Appendix C-9 Nationwide Public Safety Broadband Network (NPSBN) Use Case Definitions, Special Notice D15PS00295, April 27, 2015. https://slidex.tips/download/appendix-c-9-nationwide-public-safety-broadband-network-npsbn-use-case-definitio.

[18] Choong, Dawkins, Greene, Theofanos, *NISTIR 8181- Incident Scenarios Collection for Public Safety Communications Research: Framing the Context of Use* NISTIR 8181, National Institute of Standards and Technology, June 2017. https://doi.org/10.6028/NIST.IR.8181.

[19] FIPS 199, *Standards for Security Categorization of Federal Information and Information System.*February 2004. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

[20] Clark et al, *Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System*, Usenix, 2011. https://www.usenix.org/legacy/event/sec11/tech/full_papers/Clark.pdf

[21] iPOWER Technologies, *Hidden Virus Discovered in Martel Police Body Camera,* November 2015. http://www.goipower.com/?pageId=40 [accessed 11/19/2017].

[22] Goodin, Dan, *Police body cams found pre-installed with notorious Conflicker worm, ars TECHNICA,* November 2015. https://arstechnica.com/security/2015/11/police-body-cams-found-pre-installed-with-notorious-conficker-worm/ [accessed 11/19/2017].

[23] Williams, Clarence, *Hackers hit D.C. police closed-circuit camera network, city officials disclose,* The Washington Post, January 2017. https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html?utm_term=.748cdb7c66ed [accessed 11/20/17].

[24] PoliceOne Staff, *DC police: Cyberattack affects surveillance cams before inauguration*, PoliceOne.com, January 2017. https://www.policeone.com/police-products/radios/surveillance/articles/284874006-DC-police-Cyberattack-affected-surveillance-cams-before-inauguration/ [accessed 11/20/17].

[25] Boots, Michelle, *Anchorage will end public broadcast of police, fire radio communication,* Anchorage Daily News, August 2016. https://www.adn.com/alaska-news/crime-courts/2016/08/08/anchorage-will-end-public-broadcast-of-police-fire-radio-communication/#3840 [accessed 11/20/17].

[26] Association of Public-Safety Communications Officials (APCO) International, home page. https://www.apcointl.org [accessed 11/20/17].

[27] Rupar, Aaron, *Teens face felonies after allegedly stealing cop radio and broadcasting, "F**k the police",* City Pages, June 2012. http://www.citypages.com/news/teens-face-felonies-after-allegedly-stealing-cop-radio-and-broadcasting-fk-the-police-6534079 [accessed 11/20/17].

[28] Hamilton, Matt, *LAPD officer charged with stealing police radio, failing to pay for baby stroller: 'We trusted her because she was a police officer',*Los Angeles Times, August 2016. http://www.latimes.com/local/lanow/la-me-ln-lapd-officer-charged-20160829-snap-story.html [accessed 11/20/17].

[29] Kirby, Jen, *Somebody Hacked the NYPD Police Radio to Make Threats to an Officer,* Daily Intelligencer, August 2016. http://nymag.com/daily/intelligencer/2016/08/somebody-hacked-nypd-radio-to-threat-cops-yodel.html [accessed 11/20/17].

[30] The Cardinal, *Police Radio Encryption: Not Secure, A Transparency Failure, A Public Safety Nightmare*, ArlingtonCardinal.com, December 2012. http://www.arlingtoncardinal.com/2012/12/police-radio-encryption-not-secure-a-transparency-failure-a-public-safety-nightmare/ [accessed 11/20/17].

[31] Payne, Stewart, *Ooh Betty, I've got a stolen police radio,* The Telegraph, August 2003. http://www.telegraph.co.uk/news/uknews/1439383/Ooh-Betty-Ive-got-a-stolen-police-radio.html [accessed 11/20/17].

[32] Wiquist, Will, *FCC FINES FLORIDA DRIVER $48,000 FOR JAMMING CELLULAR & PUBLIC SAFETY COMMUNICATIONS DURING WORK COMMUTE,* FCC News, May 2016.

https://apps.fcc.gov/edocs_public/attachmatch/DOC-339559A1.pdf [accessed 11/20/17].

[33] Carman, Ashley, *Police arrested a hacker who allegedly triggered a DDoS attack on the 911emergency call system,* The Verge, October 2016. https://www.theverge.com/2016/10/30/13471128/meetkumar-hiteshbhai-desai-arrest-911-exploit [accessed 11/20/17].

[34] Paley, Tyler, *18-year-old arrested in cyberattack on Ariz.911 system,* USA TODAY, October 2016. https://www.usatoday.com/story/tech/nation-now/2016/10/28/911-cyberattack-phoenix-area/92886480/ [accessed 11/20/17].

[35] Hult, John, *Ex-fire division chief charged with hacking documents,* Argus Leader., September 2014. http://www.argusleader.com/story/news/city/2014/09/17/ex-fire-division-chief-charged-hacking-documents/15805819/ [accessed 11/20/17].

[36] Dunsmoor, Bren, *Fmr. SF Fire Official Admits to Hacking Chief's Email,* Keloland Media Group, December2014. http://origin-www.keloland.com/news/article/news/fmr-sf-fire-official-admits-to-hacking-chiefs-email [accessed 11/20/18].

[37] Appriss, Inc., *MobilePatrol Public Safety App,* Google Play Store, March 2017. https://play.google.com/store/apps/details?id=com.appriss.mobilepatrol&hl=en [accessed 11/20/17].

[38] Bogardus, Kevin, *Radios failed during Navy Yard attack, emergency responders say,* The Hill, September 2013. http://thehill.com/homenews/news/323495-radios-failed-during-navy-yard-attack-first-responders-say [accessed 11/20/17].

[39] Evans, Bo, *ND Information Technology Dept. says state's emergency radio systems may be failing,* KFYR-TV, February 2017. http://www.kfyrtv.com/content/news/ND-Information-Technology-Dept-says-states-emergency-radio-systems-may-be-failing-413769003.html [accessed 11/20/17].

[40] Henderson, Tim, *Attacks, Crashes Underscore Need for New 911 Systems,* The PEW Charitable Trusts, March 2017. http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2017/03/24/attacks-crashes-underscore-need-for-new-911-systems [accessed 11/20/17].

[41] Association of Public-Safety Communications Officials (APCO) International, *APCO Project 25 Statement of Requirements,* March 2010. https://www.apcointl.org/images/pdf/SOR-2010.pdf [accessed 11/19/17]

[42] U.S. Department of Homeland Security, *DHS 4300A Sensitive Systems Handbook Version 12.0,* Homeland Security, November 2015. https://www.dhs.gov/sites/default/files/publications/4300A%20Sensitive-Systems-Handbook-v12_0-508Cs.pdf [accessed 11/20/17].

[43] Association of Public-Safety Communications Officials (APCO) International, Application Community (AppCom), home page. http://appcomm.org [accessed 11/19/17].

[44] Lair, Yannick, *Mission Critical Services in 3GPP*, 3GPP A Global Initiative, June 2017. http://www.3gpp.org/news-events/3gpp-news/1875-mc_services [accessed 12/08/17]

[45] S. Quirolgico et. al., *Vetting the Security of Mobile Applications*, NIST SP 800-163, NIST, January 2015. https://doi.org/10.6028/NIST.SP.800-163.

[46] National Institute of Standards and Technology, *Special Publication (SP) 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops Rev 1*, July 2013. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

[47] 3rd Generation Partnership Project, *Security architecture and procedures for 5G System,* 3GPP TS 33.501 V15, 2018. http://www.3gpp.org/ftp/specs/archive/33_series/33.501/ [accessed 6/11/18]

[48] National Institute of Standards and Technology, *Special Publication (SP) 1108 revision 3, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0*, September 2014. http://dx.doi.org/10.6028/NIST.SP.1108r3.

[49] U.S. Department of Homeland Security United States Computer Emergency Readiness Team (US-CERT), *Technical Information Paper-TIP-10-105-01 Cyber Threats to Mobile Devices*, April 2010. https://www.us-cert.gov/sites/default/files/publications/TIP10-105-01.pdf

[50] U.S. Department of Homeland Security SAFECOM *Assuring A Safer America Through Effective Public Safety Communications.* https://www.dhs.gov/safecom/resources.

[51] U.S. Department of Homeland Security SAFECOM *DHS Announces the 2018 Rural Emergency Medical Communications Demonstration Project (REMCDP) Grant Recipient.* https://www.dhs.gov/safecom/blog/2018/09/28/2018-remcdp-grant-recipient.

[52] U.S. Department of Homeland Security Science and Technology, *First Responder Publications.* https://www.dhs.gov/science-and-technology/frg-publications.

[53] National Public Safety Telecommunications Council (NPSTC), *NPSTC Reports*. http://www.npstc.org/npstcReports.jsp.

[54] NIST Public Safety Communications Research Division, *2013 Public Safety Broadband Stakehholder Meeting,* https://www.nist.gov/ctl/pscr/2013-public-safety-broadband-stakeholder-meeting.

[55] National Telecommunications and Information Administration (NTIA),

Spectrum Engineering Reports. https://www.ntia.doc.gov/legacy/osmhome/Reports.html.

[56] National Telecommunications and Information Administration (NTIA), *Institute for Telecommunication Sciences (ITS),* https://www.ntia.doc.gov/category/institute-telecommunication-sciences.

[57] National Institute of Standards and Technology, *Special Publication (SP) 800-30 revision 1, Guide for Conducting Risk Assessments*, September 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[58] NIST Public Safety Communications Research Division, *Public Safety Mission Critical Voice,* https://www.nist.gov/ctl/pscr/research-portfolios/public-safety-mission-critical-voice.

[59] NIST National Cybersecurity Center of Excellence (NCCoE), *Mobile Application SinglenSign-On Improving Authentication for Public Safety First Responders,* April 2018. https://www.nccoe.nist.gov/sites/default/files/library/sp1800/psfr-mobile-sso-nist-sp1800-13-draft.pdf.