

**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>

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

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>

November 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

55
56National Institute of Standards and Technology Interagency Report 8196
75 pages (November 2018)57
58This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8196-draft>59
60
61
62

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.

63
64
65
66
67
68

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.

69
70
71

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>.

72

73

Public comment period: *November 30, 2018 through January 7, 2019*

74

National Institute of Standards and Technology

75

Attn: Applied Cybersecurity Division, Information Technology Laboratory

76

100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

77

Email: nistir8196@nist.gov

78

79

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

80

81 **Reports on Computer Systems Technology**

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

90 **Abstract**

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

101 **Keywords**

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

103 **Acknowledgments**

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

111 **Audience**

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

115

116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148

Table of Contents

1 Introduction 1

 1.1 Purpose 1

 1.2 Scope..... 2

 1.3 Previous Work..... 2

 1.4 Document Structure 2

 1.5 Document Conventions..... 3

2 Technology Overview 4

 2.1 Land Mobile Radio Technology..... 4

 2.2 Cellular Technology 5

 2.3 Wearable Technology 5

3 Related Standards & Guidance..... 9

 3.1 Association of Public-Safety Communications Officials 9

 3.2 Department of Homeland Security 9

 3.3 FirstNet Public Safety Advisory Committee (PSAC) 10

 3.4 National Public Safety Telecommunications Council 10

 3.5 Public Safety Communications Research 10

 3.6 NIST Information Technology Laboratory 10

 3.7 NTIA..... 10

4 Study Methodology 11

 4.1 Preliminary Research..... 11

 4.2 Public Safety Input..... 11

 4.3 Security Analysis & Objectives Development 11

5 Use Cases for Public Safety Mobile & Wearable Device Security 12

 5.1 Use Case Development Methodology..... 12

 5.2 Use Case Structure..... 12

 5.3 Mobile Device Use Cases 13

 5.4 Wearable Device Use Cases 16

 5.5 Mobile Application Use Cases 18

6 Documented Attacks on Public Safety Systems 23

 6.1 Threat Source Type Descriptions..... 23

 6.2 Adversarial Attacks 24

149	6.3 Structural & Environmental Incidents	26
150	7 Threat Analysis	28
151	7.1 Threat Analysis Methodology.....	28
152	7.2 Threats to Public Safety Mobile Devices.....	31
153	7.3 Threats to Public Safety Wearable Devices.....	42
154	7.4 Areas Warranting Further Scrutiny.....	49
155	8 Security Objectives	53
156	8.1 Availability	53
157	8.2 Ease of Management.....	54
158	8.3 Interoperability	54
159	8.4 Isolation	56
160	8.5 Confidentiality	56
161	8.6 Authentication	57
162	8.7 Integrity	58
163	8.8 Device & Ecosystem Health.....	58
164	9 Conclusions.....	60
165	List of Tables	
166	Table 1: Example Threat Event.....	28
167	Table 2: Modified Threat Source Definitions	29
168	Table 3: Potential Impact Definitions from FIPS 199.....	29
169	Table 4: Modified Threat Occurrence Definitions	31
170	Table 5: Threats to Public Safety Mobile Devices	31
171	Table 6: Threats to Public Safety Wearable Devices	42
172	Table 7: Summary of Jamming Attacks on Device Types	52
173	List of Figures	
174		
175		
176	Figure 1 - Examples of Public Safety Wearables	7
177	List of Appendices	
178		
179	Appendix A— Acronyms	62
180	Appendix B— References	64
181		

182 **1 Introduction**

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

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

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

210 **1.1 Purpose**

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

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

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

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

229 **1.2 Scope**

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

240 **1.3 Previous Work**

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

250 **1.4 Document Structure**

251 The document is organized into the following major sections:

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

260 The document also contains appendices with supporting material:

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

263 **1.5 Document Conventions**

264 The term *mobile device* is used to refer to a modern smartphone running a full-fledged operating
265 system (OS). Please refer to *NIST Special Publications (SP) 800-124 Guidelines for Managing*
266 *the Security of Mobile Devices in the Enterprise* for additional information on defining mobility
267 [4]. Mobile devices generally have cellular service, but not always. *Tablets* are traditionally
268 larger than mobile devices, run a full-fledged OS, and are typically assumed to lack cellular
269 service unless otherwise noted. The term *LMR handset* refers to a handheld communication
270 device broadly used by public safety officials in the field today. LMR handsets do not generally
271 have cellular capabilities. The term *wearable*, or *wearable device*, refers to a small device that
272 may or may not have a full-fledged OS. Wearables are generally assumed to lack cellular service
273 and rely on short-range wireless protocols like WiFi or Bluetooth, but this is not always the case.
274

275 **2 Technology Overview**

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

277 **2.1 Land Mobile Radio Technology**

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

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

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

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

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

320 **2.2 Cellular Technology**

321 A cellular network is a wireless network with a distributed coverage area made up of cellular
322 sites housing radio equipment (i.e., base stations). These base stations are often owned and
323 operated by a wireless telecommunications company. The 3rd Generation Partnership Project
324 (3GPP) is a worldwide standards development organization focused on cellular technology,
325 including 3rd Generation (3G) universal mobile telecommunication system (UMTS) and 4th
326 Generation (4G) LTE technologies. LTE networks are deployed across the globe, and
327 installations continue to increase as the demand for high-speed mobile networks is constantly
328 rising. 3GPP defines a number of high-level goals for LTE systems to meet, including:

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

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

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

349 **2.3 Wearable Technology**

350 A wearable is an IoT device that is worn on the body or as an accessory. Wearables are often
351 single-purpose embedded systems collecting data from a set of sensors built into the device. The
352 sensors can collect a wide variety of information, such as the body's current thermal temperature,
353 cardiovascular activity, or GPS location. In some instances, such as smartwatches, wearables can
354 run applications quite similar to mobile applications. These devices may or may not run a

355 traditional OS with modern security features enabled. In fact, many sensor-based devices may
356 not even run what could be considered a traditional OS.

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

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

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

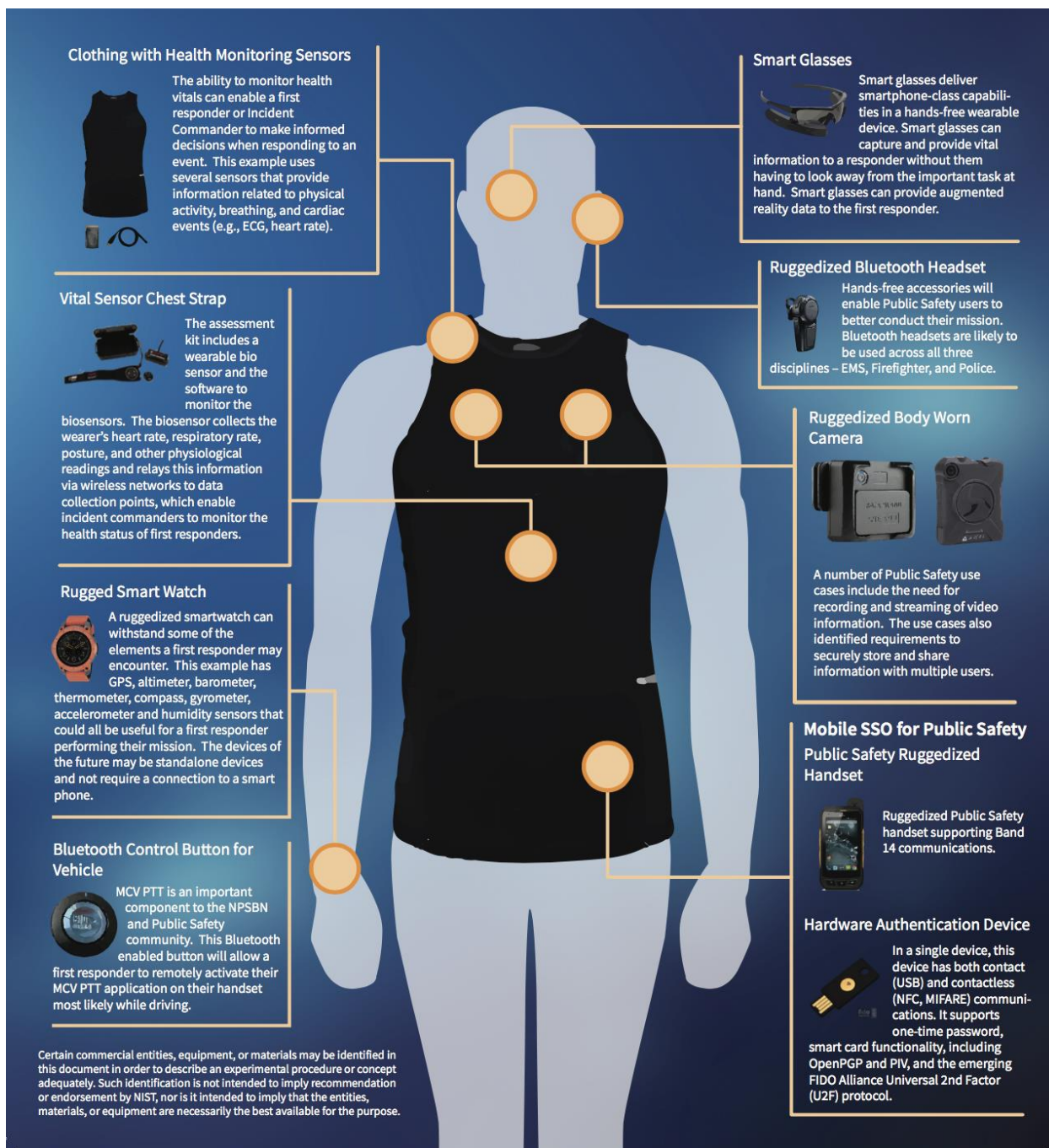


Figure 1 - Examples of Public Safety Wearables

375
376

377
378
379
380
381
382

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.

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

3 Related Standards and Guidance

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

3.1 Association of Public-Safety Communications Officials

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

3.2 Department of Homeland Security

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

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

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

430 **3.3 FirstNet Public Safety Advisory Committee (PSAC)**

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

437 **3.4 National Public Safety Telecommunications Council**

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

444 **3.5 Public Safety Communications Research**

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

450 **3.6 NIST Information Technology Laboratory**

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

455 **3.7 National Telecommunications and Information Administration**

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

465 **4 Study Methodology**

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

471 **4.1 Preliminary Research**

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

479 **4.2 Public Safety Input**

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

487 **4.3 Security Analysis and Objectives Development**

488 PSCR engineers used the preliminary research and input received from public safety
489 practitioners to perform a threat analysis and create a threat event list. A modified version of
490 NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [57] informed the risk
491 analysis methodology used to analyze each threat event, including the vulnerability, threat
492 sources, security category, likelihood, and impact. Based on this analysis, PSCR engineers
493 developed a list of security objectives and their relevance to public safety, which are described in
494 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

537 information (e.g., sensors, cameras, scanners). The application use cases include the software on
 538 the devices used to gather, process, and/or transmit information.
 539 Each use case utilizes the following format:

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

546 **5.3 Mobile Device Use Cases**

547 **5.3.1 Mobile Information Collection and Sharing**

548 *Source:* PSAC #26

549 *Technology:* public safety mobile device, backend storage location, virtual private network
 550 (VPN)

551

552 **Description**

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

559

560 **Security Concerns**

561 The data stored on the officer's mobile device and the backend storage facility may be
 562 unencrypted. The data in transit for the data transfer to the backend storage location may be
 563 unencrypted if a VPN is not utilized. The unencrypted data allows for easy access of information
 564 by unauthorized users. Lack of network availability could delay the officer from quickly
 565 transferring the missing person's information to the necessary parties and media outlets.
 566

567 **5.3.2 Shared Equipment with Multiple Users**

568 *Source:* NPSTC #2.7, SAFECOM 3.3.1, FirstNet 4.8.4

569 *Technology:* public safety mobile device, device-side user isolation technology, single sign-on
 570 services

571

572 **Description**

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

578

579 Security Concerns

580 The officer may have unauthorized access to sensitive information that was authorized for a
581 previous user. Additionally, accidentally collected PII may be exposed, and QPP values may be
582 incorrectly assigned (e.g., higher priority incorrectly assigned to a lower priority user). Location
583 data and health information may also be incorrectly associated with the previous user. The audit
584 logs for the device or applications may be inaccurate. Availability concerns exist if the single
585 sign-on (SSO) service goes down and the device needs to quickly be used for an emergency.
586

587 5.3.3 Gathering and Processing Biometric Information

588 *Source:* DHS Mobility Use Cases

589 *Technology:* public safety mobile device, biometric peripheral, VPN service, public safety
590 database

591

592 Description

593 A law enforcement officer needs to identify an individual in a remote area. They use a wearable
594 sensor to capture biometrics to facilitate the identification of the user. The information is
595 transmitted to HQ for processing. The officer receives the results, which provide improved
596 situational awareness and enable an informed action. Depending on coverage, the device may
597 operate in limited offline mode, over 802.11 wireless, LTE, or satellite communications.
598

599

599 Security Concerns

600 Data at rest protection for the information on the officer's mobile device and the associated
601 databases storing the biometric information is important to ensure that only authorized officials
602 receive the information. Data in transit protection for the biometric information is also important
603 and could be provided by encrypting the data at the application level and encrypting the
604 communications path (i.e., encrypted data and encrypted tunnel). Encrypting this data can protect
605 against unauthorized extraction or modification of the data in transit. In addition to
606 authenticating to the mobile device, the officer must be strongly authenticated to the applications
607 and backend public safety databases.
608

609 5.3.4 BYOD User

610 *Source:* PSCR Security

611 *Technology:* MDM/EMM/UEM, public safety mobile device, personal public safety mobile
612 device, Bluetooth headset

613

614 Description

615 A firefighter is responding to an emergency and utilizing their fully functional PSBN device.
616 Without warning, the PSBN device ceases to function, and the firefighter is unable to determine
617 the cause of the malfunction or put the device in an operational state. To continue their duties,
618 the firefighter uses their personal mobile device to conduct needed tasks, including downloading
619 and logging into public safety applications.
620

621 Security Concerns

622 The primary concern is that the firefighter needs to carry out their duties with a strong emphasis
623 on voice communication. The firefighter may be using an audio headset or other Bluetooth push-
624 to-talk (PTT) peripheral that may not be paired with their personal device. Another availability
625 issue is whether or not the necessary applications can be quickly configured and/or accessed on
626 their personal device. Finally, since their personal device is not professionally managed,
627 unpatched OS or application vulnerabilities may exist, putting sensitive information at risk.
628

629 5.3.5 BYOD - VDI on Tablet/Mobile Device

630 *Source:* DHS Mobility Use Cases

631 *Technology:* VDI application, backend VDI infrastructure, public safety mobile device
632

633 Description

634 A first responder requires access to disaster-specific information. The individual uses their
635 personal tablet to access agency applications through a virtual desktop infrastructure (VDI). The
636 VDI application is removed at the end of the disaster.
637

638 Security Concerns

639 Any user with access to the personal tablet may also have unauthorized access to the agency
640 applications through the VDI. The connection between the VDI mobile application and the
641 backend VDI infrastructure should require authentication and be confidentiality protected. The
642 tablet should be free of known vulnerabilities and malware. No incident data should be stored on
643 the device.
644

645 5.3.6 Lost or Stolen Device

646 *Source:* PSCR Security

647 *Technology:* Enterprise Mobility Management (EMM), public safety mobile device
648

649 Description

650 Two police officers are patrolling their assigned area on foot, searching for a person of interest.
651 One officer notices an individual and begins to actively pursue. During the chase, the officer
652 loses their mobile device. Once the suspect is apprehended, the officer realizes their phone is no
653 longer on their person and subsequently notifies the police department's device manager of the
654 device loss.
655

656 Security Concerns

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

664

665 **5.3.7 Communication Between Neighboring Jurisdictions**666 *Source:* PSCR Security Group667 *Technology:* public safety mobile device, encryption, dispatch668 **Description**

669 Police officers respond to an incident that results in an on-foot pursuit. The chase takes them
670 across county lines where they request assistance from the local police department. The counties
671 have implemented encryption on their devices; however, an open channel for dispatch is
672 accessible. The officers switch to the open channel and relay their needs. Local law enforcement
673 can receive the transmission and assist in pursuing the suspect.

674

675 **Security Concerns**

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

683

684 **5.4 Wearable Device Use Cases**685 **5.4.1 Wearable Integrated Sensor Technology**686 *Source:* PSAC #12 / NPSTC 2.12687 *Technology:* wearable health sensor, backend server, public safety mobile device

688

689 **Description**

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

698

699 **Security Concerns**

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

706

707 **5.4.2 Bodycam**708 *Source:* PSCR Security Group709 *Technology:* body camera, cloud storage platform, public safety mobile device

710

711 **Description**

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

716

717 **Security Concerns**

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

723

724 **5.4.3 Patient Monitor**725 *Source:* PSAC #17726 *Technology:* wireless vital signs monitor, laptop, GPS constellation

727

728 **Description**

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

735

736 **Security Concerns**

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

746

747 5.5 Mobile Application Use Cases

748 5.5.1 Application Dependent Devices

749 *Source:* PSCR Security Group

750 *Technology:* public safety mobile device, wearables, public safety vendor application

751

752 **Description**

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

757

758 **Security Concerns**

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

763

764 5.5.2 Sharing of CAD Information via Mobile App

765 *Source:* PSAC #39

766 *Technology:* public safety mobile device, CAD application, backend server

767

768 **Description**

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

773

774 **Security Concerns**

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

778

779 5.5.3 Patient Tracker

780 *Source:* PSAC #29

781 *Technology:* public safety mobile device, mobile patient mobile application, smart medical
782 bracelet, receiving hospital information system

783

784 **Description**

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

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

791

792 **Security Concerns**

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

797 **5.5.4 Electronic Patient Care Recording (EPCR) application**

798 *Source:* PSAC #32, SAFECOM 3.2.2

799 *Technology:* EPCR application, public safety mobile device, backend server

800

801 **Description**

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

806

807 **Security Concerns**

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

813

814 **5.5.5 EMS Database**

815 *Source:* PSAC #34

816 *Technology:* public safety mobile device, backend server, EMS database application

817

818 **Description**

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

825

826 **Security Concerns**

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

831

832 **5.5.6 Mission Critical Voice (MCV) Application**

833 *Source:* NPSTC 2.2

834 *Technology:* MCV application, public safety mobile device

835

836 **Description**

837 A large group of first responders is sweeping through a heavily wooded area on a search and
838 rescue mission. One first responder gets separated and lost. The first responder uses a wireless
839 headset to interface with the MCV application on their mobile device to call for assistance.

840 **Security Concerns**

841 The MCV application may not encrypt the data received and/or authenticate the headset to the
842 mobile device. This would allow external parties to listen to voice traffic and transmit false voice
843 traffic by posing as a first responder.

844

845 **5.5.7 Video Telemedicine Application**

846 *Source:* NPSTC 2.5

847 *Technology:* video telemedicine application, public safety mobile device with camera

848

849 **Description**

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

854

855 **Security Concerns**

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

858

859 **5.5.8 Collect Information through UE Camera**

860 *Source:* DHS Mobility Use Cases

861 *Technology:* public safety mobile device with camera, PDF converter application

862

863 **Description**

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

867

868 **Security Concerns**

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

873

874 **5.5.9 Push-To-Talk Telemedicine Application**

875 *Source:* NPSTC 2.11

876 *Technology:* push-to-talk (PTT) application, public safety tablet

877

878 **Description**

879 A paramedic needs additional assistance to treat a patient. The paramedic is unable to establish a
880 video session via their tablet and resorts to using PTT to communicate with a physician for
881 treatment guidance. The PTT application allows the physician to support the paramedic by
882 talking through the proper treatment needed to care for the patient.

883 **Security Concerns**

884 The PTT voice data may be unencrypted, allowing external third parties to listen to the traffic. If
885 unauthenticated users can access the channel, there is an increased chance of collisions on the
886 network. This could result in information loss between the paramedic and the physician. This
887 outcome may also occur if the communication path is intentionally jammed.

888

889 **5.5.10 Side-loading Application**

890 *Source:* PSCR Security Group

891 *Technology:* laptop, public safety mobile device, unsigned mobile application

892

893 **Description**

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

899

900 **Security Concerns**

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

905

906 **5.5.11 Public Records and Applications**

907 *Source:* PSCR Security Group

908 *Technology:* public safety mobile device, publicly available mobile applications

909

910 **Description**

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

915

916 **Security Concerns**

917 Malicious actors may install these applications to track public safety official's activities.

918 Although the officials' location information is not available in real-time, areas of increased

919 presence may easily be identified.

920 **6 Documented Attacks on Public Safety Systems**

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

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

930 **6.1 Threat Source Type Descriptions**

931 This section will identify and describe types of threat sources in accordance with *NIST SP 800-*
932 *30 Revision 1, Guide for Conducting Risk Assessments* [12]. The threat source types are then
933 generalized to documented attacks cited in succeeding sections.
934

935 **6.1.1 Adversarial**

936 **Abusing public data sources:** Combining and analyzing information from multiple public data
937 sources to perform a malicious activity
938

939 **Eavesdropping:** Sniffing traffic on a medium that is not confidentiality protected; the content of
940 communications may be used to perform other malicious activities
941

942 **Insider threat:** An individual with privileged access in an organization who uses such access to
943 pose a threat to the organization
944

945 **Impersonation:** An individual or entity masquerading as another, often trusted party;
946 information or actions are typically requested if the impersonator has sufficient privileges to
947 make the request
948

949 **Theft:** Information or physical items are taken without authorization
950

951 **Malware:** A program that is covertly inserted into another program with the intent to destroy
952 data, run destructive or intrusive programs, or otherwise compromise the confidentiality,
953 integrity, or availability of the victim's data, applications, or operating system [46]
954

955 **Denial of service (DoS):** Negatively affecting the availability of an information system or
956 process; similarly, distributed denial of service (DDoS) significantly affects the availability of an
957 information system or resource at scale, such as by flooding a network by simultaneously
958 sending data from various computers
959

960 **6.1.2 Accidental**

961 **Misconfiguration:** An unintentional DoS caused when an information system is not utilizing the
962 proper system, application, or user settings
963

964 **6.1.3 Failure of Controls**

965 **Equipment Failure:** Occurs when a device is unable to perform its normal activities
966

967 **6.1.4 Environmental**

968 **Natural and man-made disasters:** A natural or man-made event which causes damage to
969 physical and computer infrastructure
970

971 **6.2 Adversarial Attacks**

972 The following are attacks that exemplify a malicious external entity actively exploiting a
973 vulnerability. Each attack identifies with an adversarial threat source.
974

975 **6.2.1 Malware pre-Installed on police body cameras**

976 The Win32/Conficker.B!inf malware was found pre-installed on the police body camera
977 manufactured by Martel Electronics [21]. Conficker, as it is colloquially known, was one of the
978 most successful malware campaigns ever conducted. On the device itself, Conficker affected
979 battery performance before spreading to other information systems. In the context of public
980 safety, connections were made to other public safety mobile devices, equipment, and backend
981 traditional systems located in headquarters [22]. Much of the evidence surrounding this infection
982 points to a supply chain issue.
983

984 *Threat Source:* Adversarial – Malware

985 *Impact:* Availability
986

987 **6.2.2 Ransomware infecting police surveillance equipment**

988 In 2017, days before the 58th presidential inauguration was held in Washington D.C.,
989 approximately 70% of the storage devices used to store footage for the Metropolitan Police
990 Department's video surveillance system were infected with ransomware [24]. The system was
991 unable to function properly, and city officials subsequently took the devices offline from January
992 12-15, 2017, during which time the ransomware was removed, and the systems were rebooted.
993 Washington, D.C. officials stated that this attack was limited to closed circuit TV systems and
994 did not further affect capital city government networks [23]. It remains unclear how the cameras
995 were initially infected.
996

997 *Threat Source:* Adversarial – Malware

998 *Impact:* Availability

999 **6.2.3 Unencrypted police communications**

1000 In 2012, public safety officials in Anchorage, Alaska transmitted unencrypted voice traffic
1001 suggesting that a high school student had a gun in a classroom. Media outlets tweeted about it
1002 before police arrived at the scene and could have potentially compromised the safety of the
1003 students, teachers, and public safety officials. This launched a discussion surrounding the
1004 benefits and drawbacks of using unencrypted police voice traffic. In 2016, public safety
1005 transmissions were taken off the air after a string of robberies in Anchorage. City public officials
1006 worried that criminals were using mobile scanner apps to their tactical advantage. For instance,
1007 an individual stole a rental car in February 2016 and was quickly arrested. Following the arrest,
1008 the officer taking the stolen car in for processing heard a delayed transmission that the officer
1009 would be pulling the man over. Anchorage public safety organizations no longer broadcast
1010 unencrypted radio traffic [25].

1011

1012 *Threat Source:* Adversarial – Eavesdropping

1013 *Impact:* Confidentiality

1014

1015 **6.2.4 LMR devices stolen**

1016 In April of 2012, teens in Dilworth, Minneapolis came across an unlocked police vehicle and
1017 stole the contents, including bulletproof vests, weapons, ammunition, and radios [27]. After
1018 transmitting profanity on police frequencies, the teenagers called authorities because the
1019 handcuffs were stuck on one of the individuals. The teenagers told the police that the radio was
1020 tossed into a lake and was ultimately not recovered.

1021

1022 *Threat Source:* Adversarial – Theft

1023 *Impact:* Availability

1024

1025 **6.2.5 Reporting fake information and issuing personal threats**

1026 In 2016, an individual in Manhattan, New York began routinely broadcasting fake incidents and
1027 police shootings on NYPD-only radio frequencies, culminating in targeted threats against a
1028 specific police officer [29] [30] [31].

1029

1030 *Threat Source:* Adversarial – Impersonation

1031 *Impact:* Integrity

1032

1033 **6.2.6 Jamming police transmissions**

1034 In 2016, a man in Tampa, Florida was fined \$48,000 for using a wireless jamming device in his
1035 car during a daily commute. The device was built to disrupt cellular transmissions and routinely
1036 affected police voice traffic [32].

1037
1038 *Threat Source:* Adversarial – Denial of Service
1039 *Impact:* Availability

1040 **6.2.7 Mobile devices unwittingly used to launch an attack**

1041 In September 2016, an 18-year-old teenager named Meetkumar Hiteshbhai Desai posted a link to
1042 Twitter that was intended to force pop-ups to appear and require users to reboot their devices
1043 [33]. Instead, the exploit caused mobile devices to continuously call 9-1-1 and hang up by
1044 activating automatic dial services. Over 1,000 Twitter users clicked the link. The attack flooded
1045 the PSAP call system and significantly slowed the call center’s response rate [34]. Updating the
1046 device’s firmware would later patch this specific 911 DDoS vulnerability.

1047
1048 *Threat Source:* Adversarial – Denial of Service
1049 *Impact:* Availability
1050

1051 **6.2.8 Unauthorized access at fire station**

1052 In 2014, a former fire rescue division chief in Sioux Falls, South Dakota was convicted of 15
1053 counts of hacking. He unlawfully used department computers to obtain unauthorized access to an
1054 email between the city and Fire Captain Michael Gramlick, spreadsheets titled “SWAT callouts,”
1055 a document titled “paystub,” and two photos [35].

1056
1057 *Threat Source:* Adversarial – Insider Threat
1058 *Impact:* Confidentiality
1059

1060 **6.2.9 Combing and presenting law enforcement information via an app store**

1061 The Google Play store hosts a mobile public safety app that can be used by malicious users to
1062 track arrests made by law enforcement [37]. The app lists data on individuals who were arrested
1063 and jailed, as well as the applicable charges. Other descriptive information about the arrested
1064 individuals is also identified.

1065
1066 *Threat Source:* Adversarial – Abusing public data sources
1067 *Impact:* Confidentiality
1068

1069 **6.3 Structural and environmental incidents**

1070 The following is a collection of incidents in which the security of public safety systems was
1071 threatened but no malicious entity necessarily exists. These incidents identify with structural
1072 threat sources.
1073

1074 6.3.1 Radio failure and interference

1075 During the active shooter incident at Washington’s Navy Yard, federal firefighter and police
1076 officer radios failed. The presence of multiple mobile command centers and a lack of centralized
1077 coordination hampered communication. Devices worked initially, but as emergency responders
1078 ventured deeper into the building where the shooting occurred, radios stopped functioning. The
1079 Incident Commander inside the building could not communicate with those outside of the
1080 building. Individual emergency responders eventually had to use cellphones and other ad hoc
1081 communication mechanisms [38].

1082 *Threat Source:* Structural – Equipment failure

1083 *Impact:* Availability

1084

1085 6.3.2 Inoperable communications systems

1086 A study conducted by the North Dakota Information and Technology Department in 2014
1087 revealed several reliability issues with the state’s radio system, which suffers from coverage
1088 issues and dead zones [39].

1089

1090 *Threat Source:* Structural – Equipment failure

1091 *Impact:* Availability

1092

1093 6.3.3 Service disruptions to the 911 system

1094 In March 2017, AT&T wireless customers in seven states were unable to reach 911 due to a
1095 “service issue” that the Federal Communications Commission is still investigating [40].

1096

1097 *Threat Source:* Structural – Equipment failure

1098 *Impact:* Availability

1099 **7 Threat Analysis**

1100 The following section describes the threat analysis performed for public safety mobile devices
1101 and wearables. This information can be used to construct a preliminary threat model for this class
1102 of information systems. The methodology used to conduct this analysis is detailed below.

1103 **7.1 Threat Analysis Methodology**

1104 Each threat listed is considered using the scenario of a medium-sized jurisdiction responding to
1105 an emergency. Threats are considered within the context of EMS, fire service, and law
1106 enforcement. Characteristics are identified and noted for each threat, all of which are defined
1107 below. These characteristics include the threat event, vulnerability, threat source, impact
1108 category, likelihood, and severity.

1109 Threat events are divided into two major technology categories: those affecting mobile devices
1110 and those affecting wearables, each of which are described in separate sections. Threat events
1111 were initially taken from the information contained within the use cases and previously identified
1112 attacks sections. All threat events are scoped directly to the mobile and wearable devices, which
1113 does not include the networks they are connected to or any backend systems. All threat events
1114 are initially presented in the following manner and followed by a detailed description of the
1115 threat.
1116

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

1117
1118 A *threat event* is defined as any event or situation with the potential of causing undesirable
1119 consequences or impact. For example, the loss of radio communications is a threat event for
1120 public safety systems. It is important to note that humans are not the only cause of threat events;
1121 natural disasters and equipment failures are potential threat events, particularly to the availability
1122 of systems.

1123 A *vulnerability* is a weakness in a process or system. This weakness could reside within a set of
1124 procedures, internal control, or system implementation that could be exploited by a threat source.
1125 A *threat source* is the adversary intending to exploit a vulnerability or a situation that may
1126 accidentally or incidentally exploit a vulnerability. The threat sources used within this analysis
1127 are adapted from the list of threat sources defined within NIST SP 800-30 Revision 1, *Guide for*
1128 *Conducting Risk Assessments* [12], which include:
1129

1130

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

1131

1132

1133

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.

1134

1135

1136

1137

1138

1139

1140

1141

1142

1143

1144

1145

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 breached. 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.

<p>Availability Ensuring timely and reliable access to and use of information [44 U.S.C., SEC. 3542]</p>	<p>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.</p>	<p>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.</p>	<p>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.</p>
---	---	---	--

1146
1147
1148
1149
1150

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:

1151
1152
1153
1154
1155
1156
1157
1158
1159
1160

- **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.

1161
1162

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.

1163
1164
1165
1166
1167
1168
1169
1170

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]*:

1171

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

1172

1173 **7.2 Threats to Public Safety Mobile Devices**

1174 The following threats concern the use of public safety mobile devices.

1175

1176

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

1177

1178 **7.2.1 Sensitive information is intercepted from a mobile device**

1179 **Threat Description:** A malicious entity eavesdropping on public safety traffic during an
1180 emergency situation

1181

1182 **Vulnerability:** Several distinct vulnerabilities could be exploited in this instance. The simplest
1183 vulnerability is a lack of encryption for the data path used by the mobile device, including
1184 cellular, WiFi, and Bluetooth. Additionally, broken cryptographic algorithms and insufficient
1185 key sizes could also be used, which could then be broken in order to access plaintext content of
1186 communications.

1187

1188 **Threat Source:** Adversarial

1189

1190 **Likelihood:** High

1191 *Justification:* Police scanner applications are available in most app stores, and commercially
1192 available equipment allows individuals to easily listen to unencrypted public safety
1193 communications.

1194

1195 **Severity - Emergency Medical Service:** Moderate Confidentiality Impact

1196 *Justification:* This information could contain personal details about patients, such as first name,
1197 last name, address, insurance information, medical history, and current injuries, all of which is
1198 subject to HIPAA regulations. This would be unlikely to result in a loss of human life.

1199

1200 **Severity - Fire Service:** Low Confidentiality Impact

1201 *Justification:* An adversary with access to this information would be unlikely to pose a threat to a
1202 firefighter's immediate survival of the emergency situation at hand.

1203

1204 **Severity - Law Enforcement:** High Confidentiality Impact

1205 *Justification:* The classification of this data depends on the type of incident at hand. The high
1206 impact level is assigned because there exists the possibility of loss of life. For instance, sensitive
1207 information shared at a crime scene or an undercover officer simply communicating with law
1208 enforcement could lead to loss of life. It is of note that much of a law enforcement officer's
1209 routine communication is sent securely, making this classification situation-dependent.

1210

1211 **Source:** Use Case – Mobile Information Collection and Sharing; Known Attacks – Unencrypted
1212 Police Communications in Anchorage, Alaska

1213

1214 **Mitigations:**

1215 Cryptography can be used to provide confidentiality protection for public safety
1216 communications. Encryption can be implemented by the network to simplify algorithm selection
1217 and cryptographic key management issues. Encryption could also be provided by an application,
1218 which would then use the network as a simple data transport mechanism. In this instance, if the
1219 network is also encrypting traffic, information may be encrypted twice. This may cause lower
1220 data throughput but may be necessary for disciplines and situations requiring confidential
1221 communications.

1222

1223 **7.2.2 Accidental disclosure of information via a shared device or resource**

1224 **Threat Description:** In many cases, public safety practitioners share a pool of available radios.
1225 This practice may continue with mobile devices, and an information disclosure could occur if an
1226 individual reuse a mobile device and finds themselves already logged into services and resources
1227 used by a colleague. For instance, the new user may be able to access pictures taken by the
1228 previous user. Currently, there is no convenient or fully functional means of signing out of all
1229 applications that are in use.

1230

1231 **Vulnerability:** This situation allows for a lack of or improperly implemented access controls,
1232 including both local and remote authentication. In terms of local authentication, the lack of a

1233 lockscreen could allow this information disclosure to occur. For remote authentication, a
1234 persistent session that does not log out after a pre-determined period could compromise
1235 confidentiality of the data.

1236
1237 **Threat Source:** Accidental

1238
1239 **Likelihood:** Moderate

1240 *Justification:* Users may not regularly log out of personal services, meaning this occurs
1241 frequently.

1242
1243 **Severity - Emergency Medical Service:** Low Confidentiality Impact

1244 *Justification:* Patient information is unlikely to be exposed in this instance as these databases
1245 often require additional levels of authentication.

1246 **Severity - Fire Service:** Low Confidentiality Impact

1247 *Justification:* Exposed information is likely to be personal in nature rather than sensitive public
1248 safety information.

1249
1250 **Severity - Law Enforcement:** Moderate Confidentiality Impact

1251 *Justification:* Mature access controls are already in place for databases that host criminal and
1252 other sensitive law enforcement information. Unsecured information here would only be
1253 accessed by members of law enforcement and not disclosed to the public, lessening the impact.

1254
1255 **Source:** Use Case – Shared Equipment with Multiple Users

1256
1257 **Mitigations:**

1258 Authenticating a specific user to devices and applications before granting access would be a
1259 useful control to prevent this type of data spillage. Some smartphones already contain multi-user
1260 functionality that could be extended to accommodate the need to share devices. Further research
1261 in this area is being conducted at the National Cybersecurity Center of Excellence (NCCoE).

1262

1263 **7.2.3 Individual accesses information and services via a lost or stolen public safety** 1264 **device**

1265 **Threat Description:** Lost or stolen devices can allow potentially malicious individuals to access
1266 sensitive public safety information. Even with lockscreen authentication, some public safety
1267 information may be exposed. For instance, notifications from cellular services (e.g., text
1268 messages, missed calls) or installed apps may be shown on the lockscreen.

1269
1270 **Vulnerability:** This situation is impacted by the lack of or improperly implemented access
1271 controls, including both local and remote authentication. In terms of local authentication, the lack
1272 of a lockscreen could allow this information disclosure to occur. For remote authentication, a
1273 persistent session that does not log out after a pre-determined period could compromise
1274 confidentiality of the data.

1275
1276 **Threat Source:** Adversarial, Human error

1277

1278 **Likelihood:** Moderate
1279 *Justification:* Public safety devices may be lost or stolen with the same frequency as commercial
1280 and enterprise devices.

1281
1282 **Severity - Emergency Medical Service:** Moderate Confidentiality Impact
1283 *Justification:* Patient information is unlikely to be exposed in this instance as these databases
1284 often require additional levels of authentication.

1285
1286 **Severity - Fire Service:** Low Confidentiality Impact
1287 *Justification:* PII or other sensitive information is unlikely to be exposed.

1288
1289 **Severity - Law Enforcement:** High Confidentiality Impact
1290 *Justification:* The exposed information could be quite sensitive with regard to ongoing
1291 emergency incidents.

1292 **Source:** Use Case – Lost or Stolen Device; Known Attacks – LMR Device Stolen

1293
1294 **Mitigations:**
1295 Properly configured mobile devices that authenticate users or roles before providing access to
1296 sensitive information can prevent unauthorized access. For local authentication, a proximity
1297 token could be used. For instance, if an officer's badge contains a proximity token, and their
1298 badge is physically separated from the phone, the phone automatically locks and requires further
1299 authentication. Other forms of authentication may include biometric or behavioral authentication
1300 methods. In terms of mitigations for remote authentication scenarios, time-based session logouts
1301 and regular reauthentication may be useful.

1302

1303 **7.2.4 Pre-installed spyware on device accesses sensitive data**

1304 **Threat Description:** Spyware or other malware could be installed and shipped with a device,
1305 compromising the device before it is even activated or provisioned. Spyware could monitor how
1306 the device is used and forward information to a bad actor [7].

1307
1308 **Vulnerability:** Lack of supply chain mitigations that would ensure that only properly sourced
1309 software and hardware are used in the public safety mobile device.

1310
1311 **Threat Source:** Adversarial nation-state and/or adversarial organization supplier

1312
1313 **Likelihood:** Low
1314 *Justification:* Although general malware has been seen beforehand, pre-installed malware
1315 designed specifically to affect public safety has not been witnessed.

1316
1317 **Severity - Emergency Medical Service:** Moderate Confidentiality Impact
1318 *Justification:* This information could contain personal details about patients, such as first name,
1319 last name, address, insurance information, medical history, and current injuries, all of which is
1320 subject to HIPAA regulations. This would be unlikely to result in a loss of human life.

1321

1322 **Severity - Fire Service:** Low Confidentiality Impact

1323 *Justification:* An adversary with access to this information would be unlikely to pose a threat to a
1324 firefighter's immediate survival of the emergency situation at hand.

1325
1326 **Severity - Law Enforcement:** High Confidentiality Impact

1327 *Justification:* The classification of this data depends on the type of incident at hand. The high
1328 impact level is assigned because there exists the possibility of loss of life. For instance, sensitive
1329 information shared at a crime scene or an undercover officer simply communicating with law
1330 enforcement could lead to loss of life. It is of note that much of a law enforcement officer's
1331 routine communication is sent securely, making this classification situation-dependent.

1332
1333 **Source:** Known Attacks – Malware Pre-Installed on Police Body Cameras

1334
1335 **Mitigations:**

1336 Proper consideration of risks associated with the supply chain, especially hardware
1337 manufacturers and firmware developers, may assist with ensuring the integrity of the system.
1338 This potentially includes purchasing devices from trusted vendors. Applications installed on
1339 mobile devices and wearables should be vetted. NIST SP 800-163 can assist with the vetting of
1340 mobile applications [45].

1341

1342 **7.2.5 A denial of service or other technical attack blocks communications**

1343 **Threat Description:** A variety of technical DoS attacks exist, from exploiting protocol specific
1344 vulnerabilities (e.g., WiFi disassociation frames), smart jamming attacks, and less sophisticated
1345 spectrum jamming attacks. All of these can occur for any wireless protocol, including Bluetooth,
1346 WiFi, and LTE.

1347
1348 **Vulnerability:** DoS attacks can occur when protocols are not designed to withstand jamming
1349 attacks or when there is a lack of available spectrum to use. Many technologies that will be
1350 deployed will utilize the already noisy ISM band.

1351
1352 **Threat Source:** Adversarial, Accidental

1353
1354 **Likelihood:** Moderate

1355 *Justification:* This may accidentally occur often, as many technologies used here may utilize the
1356 ISM band.

1357
1358 **Severity - Emergency Medical Service:** High Availability Impact

1359 *Justification:* The inability to relay information to the appropriate parties or call for help could
1360 lead to loss of life.

1361
1362 **Severity - Fire Service:** High Availability Impact

1363 *Justification:* Firefighters being unable to communicate during an emergency fire situation could
1364 lead to loss of life of either the firefighter or the victim.

1365

1366 **Severity - Law Enforcement:** High Availability Impact
 1367 *Justification:* This could lead to loss of life if a police officer responds to a situation, is wounded,
 1368 and is unable to call for help.

1369
 1370 **Source:** Known Attacks – Jamming police Transmissions in Tampa, FL; Known Attacks –
 1371 DDoS of Emergency 911 System

1372
 1373 **Mitigations:**
 1374 Using wireless communication protocols that are more resistant to dumb and smart jamming
 1375 attacks, such as frequency-hopping spread spectrum (FHSS). Certain protocols are more resistant
 1376 to protocol jamming than others and should be carefully considered before implementation.
 1377 Wired devices and earpieces may be useful but will ultimately need to connect to a wireless
 1378 device that may be vulnerable to these types of attacks.

1379

1380 7.2.6 Structural or architectural issues interference

1381 **Threat Description:** Structures or other environments that public safety personnel may venture
 1382 into as part of their work may not allow cellular and other signals to properly penetrate.

1383 **Vulnerability:** Radio frequencies lack sufficient signal strength to penetrate the environment,
 1384 and public safety personnel operate in enclosed environments.

1385

1386 **Threat Source:** Failure of controls

1387

1388 **Likelihood:** High

1389 *Justification:* Structures and surrounding environments are some of the most common causes of
 1390 interference. The density of materials, such as concrete and steel, can weaken or block radio
 1391 signals.

1392

1393 **Severity - Emergency Medical Service:** High Availability Impact

1394 *Justification:* The inability to relay information to the appropriate parties or call for help could
 1395 lead to loss of life.

1396

1397 **Severity - Fire Service:** High Availability Impact

1398 *Justification:* Firefighters may go into a burning structure with or without solid communications
 1399 in place. Being unable to communicate during an emergency fire situation could lead to loss of
 1400 life of either the firefighter or the victim.

1401

1402 **Severity - Law Enforcement:** High Availability Impact

1403 *Justification:* During an active shooter event, law enforcement must be able to relay critical
 1404 information to fellow responders both inside and outside of the building. A lack of
 1405 communications could result in additional casualties, loss of life, or other threats to public
 1406 safety.

1407

1408 **Source:** Known Attacks – Washington, D.C. Navy Yard Radio Failure

1409

Mitigations:

1411 Mobile devices can use wireless frequencies that better penetrate walls and common building
1412 materials. Repeaters and other communication technology that allow information to be chained
1413 to an external source of connectivity can assist in providing a consistent line of communication.
1414 Research of indoor coverage is ongoing within the Mission Critical Voice (MCV) portfolio at
1415 PSCR [58]. This research may assist in resolving the structural threat to mobile devices.
1416

7.2.7 Unreliable communications channel due to interoperability issues

1418 **Threat Description:** Public safety jurisdictions utilize a specific set of channels for
1419 communications. In an emergency, neighboring jurisdictions may be called in to assist. The
1420 radios of different jurisdictions may not be configurable to use the same channels, and this could
1421 disrupt communication.
1422

1423 **Vulnerability:** Disparate technology configurations across jurisdictions may not be
1424 interoperable.
1425

1426 **Threat Source:** Failure of Controls

1427 **Likelihood:** Moderate

1428 *Justification:* While this threat does exist, jurisdictions typically designate a separate channel or a
1429 set of radios to distribute to outside public safety personnel at the scene of an incident.
1430

1431 **Severity - Emergency Medical Service:** Availability Moderate Impact

1432 *Justification:* While alternate options for communication would allow EMS responders to
1433 perform tasks and communicate with their local jurisdiction, communication may still be limited.
1434

1435 **Severity - Fire Service:** Moderate Availability Impact

1436 *Justification:* This could cause availability issues, especially with the user interface, if
1437 firefighters must switch to alternate communications channels that require a fair degree of
1438 configuration.
1439

1440 **Severity - Law Enforcement:** Moderate Availability Impact

1441 *Justification:* Limitations to device channel configuration could cause communication issues,
1442 though law enforcement officers can still retain some instance of communication to actively
1443 respond to an emergency.
1444

1445 **Source:** Known Attacks – Antiquated and Inoperable Communication Systems
1446

Mitigations:

1448 Mobile devices can use interoperable communications equipment, protocols, and security
1449 technologies. In fact, the use of LTE technology mitigates several the interoperability issues
1450 traditionally associated with LMR. Having a pre-specified method for communications fallback
1451 may provide a means of communication if there is an incompatibility issue. A jurisdiction may
1452 need to allocate a supply of devices to distribute when external jurisdictions do not have
1453 interoperable devices.
1454

1455 7.2.8 Device failure due to a lack of ruggedization

1456 **Threat Description:** A device not designed for resistance to harsh environments could fail,
1457 leaving the public safety official without a means of communication.

1458
1459 **Vulnerability:** Components of the mobile device may not be rated to handle extreme hot and
1460 cold temperatures, exposure, or submersion in liquid.

1461
1462 **Threat Source:** Environmental, Human error

1463
1464 **Likelihood:** Low

1465 *Justification:* Public safety practitioners would likely try to use public safety-grade, ruggedized
1466 devices where possible.

1467
1468 **Severity - Emergency Medical Service:** High Availability Impact

1469 *Justification:* Being unable to relay information to the appropriate parties or call for help could
1470 lead to a loss of life.

1471 **Severity - Fire Service:** High Availability Impact

1472 *Justification:* Firefighters' inability to communicate in an emergency fire situation could result in
1473 loss of life to either the firefighter or the victim.

1474
1475 **Severity - Law Enforcement:** High Availability Impact

1476 *Justification:* This could lead to loss of life if a police officer responds to a situation, is wounded,
1477 and is unable to call for help.

1478
1479 **Source:** N/A

1480
1481 **Mitigations:**

1482 The use of devices resistant to external sources of stress, such as temperature, liquid, or shock,
1483 can ensure reliability during an emergency. The International Protection Marking standard (IEC
1484 60529), informally known as the Ingress Protection (IP) rating system, measures a smartphone's
1485 resistance to water, dust, and other particles and may be a useful when evaluating devices.

1486 Although this is a serious issue, it is included for awareness and is considered outside of the
1487 scope of PSCR's research activities.

1488

1489 7.2.9 Mobile device is infected with malware resulting in a loss of sensitive information

1490 **Threat Description:** Public safety mobile devices could be attacked by mobile malware, which
1491 may store and relay public safety information to malicious entities.

1492
1493 **Vulnerability:** The device can be exposed to malicious users through a lack of OS and/or
1494 application updates, poor implementation of software assurance concepts by the developer, and
1495 inadequate application vetting tools and procedures for device apps.

1496
1497 **Threat Source:** Adversarial

1498

1499 **Likelihood:** Moderate

1500 *Justification:* Although malware is common on mobile devices, developers often resolve
1501 malware issues and send patches or updates to the mobile devices or applications. Typically, a
1502 mobile device is not vulnerable to known malware for long.

1503

1504 **Severity - Emergency Medical Service:** Moderate Confidentiality Impact

1505 *Justification:* This information could contain personal details about patients, such as first name,
1506 last name, address, insurance information, medical history, and current injuries, all of which is
1507 subject to HIPAA regulations. This would be unlikely to result in a loss of human life.

1508

1509 **Severity - Fire Service:** Low Confidentiality Impact

1510 *Justification:* An adversary with access to this information would be unlikely to pose a threat to a
1511 firefighter's immediate survival of the emergency situation at hand.

1512

1513 **Severity - Law Enforcement:** High Confidentiality Impact

1514 *Justification:* The classification of this data depends on the type of incident at hand. The high
1515 impact level is assigned because there exists the possibility of loss of life. For instance, sensitive
1516 information shared at a crime scene or an undercover officer simply communicating with law
1517 enforcement could lead to loss of life. It is of note that much of a law enforcement officer's
1518 routine communication is sent securely, making this classification situation-dependent.

1519

1520 **Source:** Known Attacks – Unauthorized Access at Fire Station

1521

1522 **Mitigations:**

1523 Mobile management solutions may assist with automated patching or by notifying the user of
1524 security patches and updates that should be routinely monitored and implemented. Software and
1525 firmware developers, in particular, should give proper consideration to risks associated with the
1526 supply chain. Applications installed on public safety mobile devices and wearables should be
1527 properly vetted before installation and use. Mobile threat defense technology can also help
1528 identify certain applications as malware, and NIST SP 800-163 [45] can assist with the vetting of
1529 mobile applications.

1530

1531 **7.2.10 Location tracking of a public safety mobile device**

1532 **Threat Description:** Mobile devices may inadvertently relay identifying information about itself
1533 through WiFi or LTE identifiers. Additionally, public safety devices may be purchased in bulk
1534 with a hardware address range that may be known by malicious actors. Finally, installed
1535 applications could programmatically access a device's location information.

1536

1537 **Vulnerability:** Many wireless protocols and devices regularly transmit unencrypted permanent
1538 identities that can be stored and tracked. Applications may access and retrieve a mobile device's
1539 location.

1540

1541 **Threat Source:** Adversarial

1542

1543 **Likelihood:** Moderate
1544 *Justification:* COTS WiFi, Bluetooth, and LTE devices regularly expose this information. If a
1545 public safety device is being used in a BYOD scenario, it is much more likely that a malicious or
1546 dangerous application is installed.

1547
1548 **Severity - Emergency Medical Service:** Low Confidentiality Impact
1549 *Justification:* Being able to track an EMT would not lead to loss of life or severely impact day-
1550 to-day operations.

1551
1552 **Severity - Fire Service:** Low Confidentiality Impact
1553 *Justification:* Being able to track a firefighter would not lead to loss of life or severely impact
1554 day-to-day operations.

1555
1556 **Severity - Law Enforcement:** High Confidentiality Impact
1557 *Justification:* If a malicious user could track an officer's device entering an area, they could
1558 evade their presence or place the officer in danger. If an undercover agent's device is targeted, it
1559 could reveal their identity and result in loss of life.

1560
1561 **Source:** N/A

1562 **Mitigations:**
1563 Randomized or obfuscated permanent identifiers can be leveraged by protocols and devices to
1564 obscure information about the mobile device's user or location. This could be accomplished
1565 using a whitelist of wireless network associations by default, followed by a move to a more
1566 typical advertisement system if devices from the whitelist are not found. Mobile Threat Defense
1567 is a product category that can help detect applications that maliciously obtain a user's location.
1568 Application vetting can help detect overzealous applications that might access this information.

1570 7.2.11 Malicious management profile or certificate is installed on a device

1571 **Threat Description:** Mobile devices can be sent special administrative requests that offer high
1572 levels of privilege on the device to a third party. These requests are known as enterprise mobility
1573 management (EMM) profiles or administrative profiles. The profiles offer some level of
1574 administrative access to the device and can provide an attacker visibility to a device user's
1575 identity and the type of device they have. Additionally, these profiles can be used to install
1576 malicious applications onto the device without going through the normal application vetting
1577 process offered by a mobile application store.

1578
1579 **Vulnerability:** First responders may unknowingly accept the profile when presented with it.
1580 Alternatively, they may choose to install free versions of paid applications.

1581
1582 **Threat Source:** Adversarial, Accidental

1583
1584 **Likelihood:** Moderate
1585 *Justification:* A malicious profile or certificate may accidentally be installed by a user who is
1586 unaware of its validity and needs immediate access to data.

1587

1588 **Severity - Emergency Medical Service:** Moderate Confidentiality Impact
 1589 *Justification:* A malicious application could glean patient information that is subject to HIPAA
 1590 regulations, including a patient’s medical history. This would be unlikely to result in a loss of
 1591 human life.
 1592
 1593 **Severity - Fire Service:** Low Confidentiality Impact
 1594 *Justification:* An adversary having access to a device or confidential information poses an
 1595 unlikely threat to a firefighter’s survival or well-being.
 1596
 1597 **Severity - Law Enforcement:** High Confidentiality Impact
 1598 *Justification:* If a malicious user could track an officer's device entering an area, they could
 1599 evade their presence or place the officer in danger. If an undercover agent's device is targeted, it
 1600 could reveal their identity and result in loss of life.
 1601
 1602 **Source:** N/A
 1603
 1604 **Mitigations:**
 1605 Appropriate training can enable users to identify legitimate enterprise mobility management
 1606 profiles, though IT staff may wish to be the only party that can accept and install them. Mobile
 1607 threat defense technology can also help identify known malicious MDM profiles. At the time of
 1608 this writing, MDM profiles can generally only have one profile installed on a device at a time.
 1609 Therefore, an agency or organization that is already using MDM profiles may already have a
 1610 mitigation in place.
 1611

1612 **7.3 Threats to Public Safety Wearable Devices**

1613 The following threats pertain to the use of public safety wearable devices.
 1614
 1615

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

1616

1617 **7.3.1 Sensitive information is intercepted from a wearable device**

1618 **Threat Description:** A malicious entity eavesdrops on public safety traffic during an emergency
1619 situation. This threat includes sniffing Bluetooth microphones and earpieces and using sensors to
1620 monitor medical information.

1621
1622 **Vulnerability:** Wearables tend to have weaker operating systems and insufficient patching
1623 mechanisms. This leaves wearables susceptible to several distinct vulnerabilities that could be
1624 exploited. The simplest vulnerability is a lack of encryption for the data path used by the mobile
1625 device, including cellular, WiFi, and Bluetooth. Additionally, broken cryptographic algorithms
1626 and insufficient key sizes could also be used to access plaintext content of communications.

1627
1628 **Threat Source:** Adversarial

1629
1630 **Likelihood:** Low

1631 *Justification:* Adversaries would need to be close in proximity to the wearable devices.

1632
1633 **Severity - Emergency Medical Service:** Moderate Confidentiality Impact

1634 *Justification:* A malicious application could glean patient information that is subject to HIPAA
1635 regulations, including a patient’s medical history. This would be unlikely to result in a loss of
1636 human life.

1637
1638 **Severity - Fire Service:** Low Confidentiality Impact

1639 *Justification:* An adversary having access to a device or confidential information poses an
1640 unlikely threat to a firefighter’s survival or well-being.

1641

1642 **Severity - Law Enforcement:** High Confidentiality Impact

1643 *Justification:* If a malicious user could track an officer's device entering an area, they could
1644 evade their presence or place the officer in danger. If an undercover agent's device is targeted, it
1645 could reveal their identity and result in loss of life.

1646
1647 **Source:** Use Case – Wearable Integrated Sensor Technology; Use Case – Bodycam; Use Case –
1648 Patient Monitor

1649
1650 **Mitigations:**

1651 Cryptography can be used to provide confidentiality protection for public safety
1652 communications. If the wearable devices have a cellular radio, encryption can be implemented
1653 by the network, which simplifies algorithm selection and cryptographic key management issues.
1654 Unlike mobile devices, current wearable devices rarely have cellular radios. This may restrict the
1655 type of algorithms and length of key sizes. For more complicated wearables, encryption could
1656 also be provided by a third-party application, but this is not commonly available.

1657

1658 **7.3.2 Malicious user spoofs wearable device and sends false information**

1659 **Threat Description:** An individual may be able to send false sensor information or other data
1660 that may be trusted by a mobile device.

1661 **Vulnerability:** A lack of integrity protection or mutual authentication protocols can lead to
1662 compromised data.

1663

1664 **Threat Source:** Adversarial

1665

1666 **Likelihood:** Low

1667 *Justification:* This type of incident has not been recorded in the past.

1668

1669 **Severity - Emergency Medical Service:** High Integrity Impact

1670 *Justification:* If a sensor or other medical information is spoofed, an injured person could die.
1671 For instance, if the sensor says that a patient's heart is functioning properly when their heart is
1672 experiencing problems, the patient may not receive necessary treatment.

1673

1674 **Severity - Fire Service:** High Integrity Impact

1675 *Justification:* Spoofed sensor readings could lead a firefighter into an area of a burning structure
1676 that is much hotter than they initially believed, which could result in death.

1677

1678 **Severity - Law Enforcement:** Moderate Integrity Impact

1679 *Justification:* A malicious user could send a falsified message about an active shooting to law
1680 enforcement, resulting in an unnecessarily heightened response that might potentially endanger
1681 the officers or the public.

1682

1683 **Source:** Use Case – Bodycam

1684

1685 **Mitigations:**

1686 Integrity protection or digital signatures could authenticate data sources. However, such

1687 capabilities are not easily available on all wearable devices. If wearables are wirelessly
1688 connected to a larger wireless network, restricting network access would also be beneficial.
1689

1690 **7.3.3 Malware on backend public safety infrastructure prevents wearable device from** 1691 **properly functioning**

1692 **Threat Description:** Malicious software corrupts or disables backend infrastructure that is
1693 providing service to wearable devices. The wearable device is not able to function without
1694 connectivity to the service.
1695

1696 **Vulnerability:** Unpatched software or other software vulnerability can impede proper
1697 functioning of a wearable device.
1698

1699 **Threat Source:** Adversarial
1700

1701 **Likelihood:** Low

1702 *Justification:* Although attacks on backend public safety infrastructure have been documented,
1703 these attacks have not necessarily impacted the use of wearables or other communications
1704 equipment.
1705

1706 **Severity - Emergency Medical Service:** Moderate Availability Impact

1707 *Justification:* An EMS technician may place monitoring sensors on a patient and attempt to relay
1708 medical concerns to the destination hospital. If communications fail, physicians may not be
1709 prepared to treat incoming victims.
1710

1711 **Severity - Fire Service:** High Availability Impact

1712 *Justification:* Wearable sensors may be unable to relay the fact that a firefighter is in need of
1713 immediate assistance.
1714

1715 **Severity - Law Enforcement:** Low Availability Impact

1716 *Justification:* Police body cameras could cease to function due to streaming service issues.
1717 Evidence that would be useful in court may not be collected.
1718

1719 **Source:** Known Attacks – Ransomware Infecting Washington, D.C. Police Surveillance
1720 Equipment
1721

1722 **Mitigations:**

1723 Hardware manufacturers and firmware developers should give proper considerations to risks
1724 associated with the supply chain. Malware detection systems can also be deployed onto the
1725 system. Many behavioral analysis systems establish a baseline of activity before they can detect
1726 malicious activity. If malware is included as part of that baseline, it may not be noticed.
1727

1728 **7.3.4 Malicious attack on wearable that causes battery drain, overheating, or explosion**

1729 **Threat Description:** An attack on a wearable device could drain its battery, overheat the device,
1730 or cause the device to explode.

1731
1732 **Vulnerability:** Unpatched software may have known exploitable vulnerabilities.

1733
1734 **Threat Source:** Adversarial

1735
1736 **Likelihood:** Low

1737 *Justification:* This type of incident has not been recorded in the past.

1738
1739 **Severity - Emergency Medical Service:** Moderate Availability Impact

1740 *Justification:* Vital monitoring devices may cease to operate. EMS staff would not receive
1741 patient information in a timely manner, especially during a mass casualty event with multiple
1742 victims requiring attention. EMTs could resort to communicating with traditional mobile devices
1743 and medical equipment.

1744
1745 **Severity - Fire Service:** High Availability Impact

1746 *Justification:* Firefighters are dependent on their wearables in emergency situations. Since the
1747 wearables are generally embedded underneath their personal protective equipment (PPE), the
1748 failure of a throat mic or earpiece could prevent firefighters from communicating that they
1749 require immediate assistance, which could result in death.

1750
1751 **Severity - Law Enforcement:** Low Availability Impact

1752 *Justification:* Even if there is an issue with an officer's wearable device, they are still able to
1753 communicate through other means, such as a mobile device. The wearable device does not
1754 hinder the officer's ability to perform. Law enforcement officers would be able to compensate by
1755 switching to another form of communication, such as their mobile device.

1756
1757 **Source:** N/A

1758
1759 **Mitigations:**

1760 The purchasing jurisdiction can research the wearable device's software update policy as well as
1761 whether or not the manufacturer actually adhered to that policy in the past, as this does not
1762 always occur. Installing software updates is key to reducing exploitable vulnerabilities that can
1763 lead to these types of failures. If the wearable device is not updatable at all, it may not be
1764 recommended for use by public safety personnel.

1765

1766 **7.3.5 Location tracking of public safety wearables**

1767 **Threat Description:** Wearables may beacon out identifying information about the device, such
1768 as WiFi or LTE identifiers. From another perspective, installed applications could
1769 programmatically access a device's location information.

1770

1771 **Vulnerability:** A lack of temporary identities means that many wireless protocols and devices
1772 regularly transmit unencrypted permanent identities that can be stored and tracked.

1773
1774 **Threat Source:** Adversarial

1775
1776 **Likelihood:** Moderate
1777 *Justification:* COTS WiFi, Bluetooth, and LTE devices regularly expose this information.

1778
1779 **Severity - Emergency Medical Service:** Low Confidentiality Impact
1780 *Justification:* Being able to track an EMT would not lead to loss of life or severely impact day-
1781 to-day operations.

1782
1783 **Severity - Fire Service:** Low Confidentiality Impact
1784 *Justification:* Being able to track a firefighter would not lead to loss of life or severely impact
1785 day-to-day operations.

1786
1787 **Severity - Law Enforcement:** High Confidentiality Impact
1788 *Justification:* If a malicious user could track an officer's device entering an area, they could
1789 evade their presence or place the officer in danger. If an undercover agent's device is targeted, it
1790 could reveal their identity and result in loss of life.

1791
1792 **Source:** N/A

1793
1794 **Mitigations:**
1795 Randomized or obfuscated permanent identifiers can be leveraged by protocols and devices to
1796 obscure wearable information (e.g., a whitelist of wireless network associations by default
1797 followed by a move to a more typical advertisement system if devices from the whitelist are not
1798 found).

1799

1800 **7.3.6 A denial of service or other technical attack jams communications**

1801 **Threat Description:** A variety of technical DoS attacks exist, from exploiting protocol-specific
1802 vulnerabilities (e.g., WiFi disassociation frames) to smart jamming attacks and less sophisticated
1803 spectrum-jamming attacks. All of these can occur for any wireless protocol, including Bluetooth,
1804 WiFi, and LTE.

1805
1806 **Vulnerability:** The protocols used may not be designed to withstand jamming attacks or the lack
1807 of an available spectrum. Many deployed technologies will utilize the already noisy ISM band.

1808
1809 **Threat Source:** Adversarial, Accidental

1810
1811 **Likelihood:** Moderate
1812 *Justification:* This may accidentally occur often as many public safety technologies utilize the
1813 ISM band. Numerous instances have been identified of jamming attacks from adversarial threat
1814 sources.

1815

1816 **Severity - Emergency Medical Service:** High Confidentiality Impact

1817 *Justification:* Being unable to relay information to the appropriate parties or call for help could
1818 lead to loss of life.

1819

1820 **Severity - Fire Service:** High Confidentiality Impact

1821 *Justification:* Firefighters being unable to communicate during an emergency fire situation could
1822 lead to loss of life of either the firefighter or the victim.

1823

1824 **Severity - Law Enforcement:** High Confidentiality Impact

1825 *Justification:* If a police officer responds to a situation, is wounded, and is unable to call for help,
1826 this could lead to loss of life.

1827

1828 **Source:** N/A

1829

1830 **Mitigations:**

1831 Public safety personnel can use wireless communication protocols that are more resistant to
1832 dumb and smart jamming attacks, such as FHSS. Certain protocols are more resistant to
1833 protocol-jamming than others and should be carefully considered before use. Wired devices and
1834 earpieces will ultimately need to connect to a mobile device that is vulnerable to these types of
1835 attacks, as documented in the previous section (7.2.5).

1836

1837 **7.3.7 Application within wearable device is infected with malware resulting in a loss of**
1838 **sensitive information**

1839 **Threat Description:** Public safety wearable devices could be attacked by mobile malware,
1840 which may store and relay public safety information to malicious entities. Although not all
1841 wearable devices support “apps” in a manner similar to mobile devices, some more sophisticated
1842 wearables do.

1843

1844 **Vulnerability:** Lack of OS and/or application updates may expose a device to malicious users.
1845 Additionally, poor implementation of software assurance concepts by the developer and
1846 application vetting tools and procedures applied to apps may compromise a device.

1847

1848 **Threat Source:** Adversarial

1849

1850 **Likelihood:** Low

1851 *Justification:* Malware designed to execute and steal information on a wearable platform is not
1852 yet commonplace, although this may change.

1853

1854 **Severity - Emergency Medical Service:** Moderate Confidentiality Impact

1855 *Justification:* This information could contain personal details about patients, such as first name,
1856 last name, address, and insurance information. Additionally, information about a patient’s
1857 medical history and/or current injuries could be exposed, all of which is data subject to HIPAA
1858 regulations. This would be unlikely to result in a loss of human life.

1859

1860 **Severity - Fire Service:** Low Confidentiality Impact

1861 *Justification:* An adversary having access to this information would be unlikely to be a threat to a
1862 firefighter's immediate survival of the emergency situation at hand.

1863

1864 **Severity - Law Enforcement:** High Confidentiality Impact

1865 *Justification:* This classification of this data depends on the immediate type of incident at hand.
1866 The high impact level is used since there exists the possibility of loss of life. For instance,
1867 sensitive information shared at a crime scene or an undercover officer communicating with law
1868 enforcement could lead to loss of life. It is of note that much of a law enforcement officer's
1869 traffic is routinely sent in the clear, making this extremely situation-dependent.

1870

1871 **Source:** N/A

1872

1873 **Mitigations:**

1874 Proper consideration should be given to risks associated with the supply chain, especially
1875 software and firmware developers. Applications installed on public safety mobile and wearable
1876 devices should be properly vetted before installation and use. Vetting applications on IoT and
1877 wearable applications are still in infancy, and guidance may not be readily available.

1878

1879 **7.4 Areas Warranting Further Scrutiny**

1880 Following the threat analysis, two cited security problems are particularly worrisome. Each of
1881 these issues affects both mobile devices and wearables. These two issues warrant additional
1882 scrutiny and research and are detailed below.

1883 **7.4.1 Device and User Tracking**

1884 It is common knowledge that the physical location of wireless devices can be tracked. These
1885 devices are often physically placed in a user's jacket or pocket, and if the presence of the
1886 wireless device is known, the location and identity of the user may also be known. Tracking of
1887 users and their wireless devices can be a staging point for physical and digital attacks against
1888 specific public safety individuals. Wireless device tracking is possible in part because wireless
1889 devices must associate with an unknown host or controller. In the first step of this association
1890 process, a device announces ("advertises" or "beacons") its presence to other devices. These
1891 beacons may contain a permanent identifier, which could be used as an easily accessible tracking
1892 mechanism.

1893 In the case of a cellular device, the International Mobile Subscriber Identity (IMSI) would be the
1894 advertised identifier. The SA3 working group may address this advertised identifier in future
1895 deployments of 5G [47]. For the 802.11 set of WiFi protocols, the identifier would be a media
1896 access control (MAC) address. As a final example, the Bluetooth identifier would be a Bluetooth
1897 MAC address, which is generated in a different manner than a typical MAC. WiFi and cellular
1898 permanent identities are typically unique across the entire world. Bluetooth permanent identities
1899 may be unique but are often simply the WiFi MAC address of a mobile device incremented by
1900 one digit.

1901 The use of these permanent identifiers by public safety devices and wearables means that they
1902 can be tracked. This may not be relevant to some public safety disciplines (e.g., fire service,
1903 EMS), but members of law enforcement may face a different scenario. At times, the identity of a
1904 police officer needs to be a secret. It would be simple for malicious individuals to collect
1905 cellular, WiFi, and Bluetooth traffic outside of a police station for an extended period. This could
1906 be done by simply hiding an inexpensive microcomputer coupled with a power source near a
1907 police station. The device could collect these advertised identifiers for hours or days and be
1908 retrieved later once its power source is depleted. A law enforcement official simply walking near
1909 a hidden device located at a station's entrance could be enough to have their personal and public
1910 safety device IDs stored in a database. These databases could be combined with other similar
1911 databases and sold on illegal marketplaces.

1912 With a database of law enforcement officials' unique device identifiers on hand, malicious
1913 individuals would have the ability to check any IMSI or MAC address they are currently
1914 receiving against a database in real time. They would then know if any law enforcement officials
1915 are in the vicinity. Law enforcement officials operating in an undercover capacity may be
1916 revealed, and personnel could be tracked to their personal residences.

1917 However, technology exists to thwart this type of tracking, specifically the use of temporary
1918 and/or randomized identifiers such as 3GPP SA3 standardized Temporary Mobile Subscriber
1919 Identities (TMSIs) and GUTI (Globally Unique Temporary Identifiers), though these are not
1920 mandatory. WiFi and Bluetooth MAC randomization is also an option, but this may be
1921 implemented in non-standardized manner if at all. Encryption of the communications channel
1922 would not generally solve this issue as these identifiers are often unencrypted during the initial
1923 attach or pairing procedure. Additionally, wireless advertisements and beacons are generally not
1924 encrypted as these messages are intentionally broadcast for any user to view.

1925 **7.4.2 Attacks on Availability**

1926 Jamming continues to be an open, unresolved problem for the availability of wireless systems.
1927 This type of attack affects certain public safety disciplines more than others, specifically the fire
1928 service. A firefighter's life depends on constant access to voice communication services, so
1929 much so that it is a common practice for firefighters to use some version of the "buddy system"
1930 when entering a dangerous situation.

1931 In the context of this document, we consider three types of jamming: wideband spectrum
1932 jamming (i.e., dumb jamming), narrowband spectrum jamming (i.e., smart jamming) and
1933 protocol jamming. Wideband jamming affects a large swath of the electromagnetic spectrum,
1934 likely multiple bands at once. Narrowband jamming affects only a small portion of the spectrum,
1935 anywhere from the ISM band to an individual carrier frequency that could be used to send a
1936 specific message. Protocol jamming is a nebulous term used to describe availability attacks
1937 against specific protocols and often removes a specific device's network access. One could make
1938 a reasonable argument that the use of the word "jamming" in this context is incorrect.

1939 APCO P.25 has been and currently is susceptible to wideband and narrowband jamming attacks,
1940 as are most wireless systems. Protocol jamming attacks are not widely available or known for
1941 this closed wireless system. LMR uses protocols and devices that have generally avoided the

1942 type of scrutiny offered to commercial devices and protocols by the cybersecurity community.
1943 With the introduction of modern mobile devices, this is no longer the case. The wireless
1944 protocols used by modern mobile devices are also susceptible to these smart and dumb jamming
1945 attacks. Yet protocol jamming attacks are well-documented, simple attacks that require
1946 inexpensive hardware and little expertise. The following table shows how this is an increase in
1947 attack surface.
1948

1949

Table 7: Summary of Jamming Attacks on Device Types

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

1950

1951

1952

1953

1954

1955

1956

1957

1958

1959

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.

1960

1961

1962

1963

1964

1965

1966

1967

1968

1969

1970

1971

1972

1973

1974

1975

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.

1976 **8 Security Objectives**

1977 Security objectives were identified based on the analysis of interview information and the threats
 1978 existing within the defined threat model. Some objectives have associated sub-objectives that are
 1979 further elaborated upon. Each objective is introduced and mapped to any associated threats. The
 1980 following principles are presented and discussed in no particular order.

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

1981 **8.1 Availability**

1982 Availability refers to “ensuring timely and reliable access to and use of information” [10]. This
 1983 characteristic was the primary objective communicated from the interviewed public safety
 1984 personnel. Availability is a multifaceted concept and exists in a variety of forms, such as network
 1985 availability, network agility, data availability, and device availability. These sub-objectives are
 1986 discussed below.

1988 **8.1.1 Network Availability**

1989 Public safety personnel require constant access to voice and data networks to perform their
 1990 duties. Supporting networks must be able to handle high traffic during an incident without
 1991 failing. On an occasion when a network fails, failure needs to occur in a graceful manner. A
 1992 graceful shutdown may include notifying public safety professionals, so they can switch to some
 1993 other means of communication. Mobile devices may attempt to switch to a different wireless
 1994 communication technology, such as point-to-point LTE, WiFi, or possibly satellite networks.
 1995 Wearables are likely to be part of a PAN that often utilize wireless technologies that operate only
 1996 within limited distances. Bluetooth (IEEE 802.15) and WiFi (IEEE 802.11) are prime examples
 1997 but not the only possibilities. Wearable devices may also contain a cellular modem capable of
 1998 communicating over LTE.

2000 **8.1.2 Network Agility**

2001 Network agility refers to the ability to switch between available networks should one
 2002 communication method fail. This aspect of availability includes the ability to modulate to other
 2003 channels and frequencies and use other wireless technologies. For instance, if an LTE public
 2004 safety network fails, a law enforcement officer would be able to switch to a different LTE
 2005 network. If a wearable device acting as part of a Bluetooth PAN is jammed due to

2006 electromagnetic interference, the wearable may attempt to connect to WiFi and subsequently try
2007 activating an LTE radio.

2008 **8.1.3 Data Availability**

2009 This aspect of availability ensures that public safety data can acquire access when needed. For
2010 instance, bone conduction technology is a useful capability as it allows firefighters to hear voice
2011 traffic inside of a fire, which is extremely loud. This same principle can be applied to throat mics
2012 for firefighters. Data availability would also be disrupted if a public safety mobile device was
2013 attacked via ransomware. A public safety employee being unable to access data due to
2014 ransomware would violate data availability.
2015

2016 **8.1.4 Device Availability**

2017 Public safety devices must operate in harsh environments. This includes extremely hot and cold
2018 temperatures, liquid submersion, and electromagnetic interference. Devices must also be able to
2019 survive drops and withstand heavy weight while remaining operational. The level of required
2020 device availability or ruggedness is unclear at this time because there is no unified public safety
2021 standard, although several military and industry standards exist.

2022 Different public safety original equipment manufacturers (OEMs) may ship devices with
2023 different Ingress Protection (IP) ratings or resistance to shock absorption. Other device
2024 ruggedization standards exist but public safety may need to define their own standard that meets
2025 their durability needs. If possible, the device should notify public safety device owners before a
2026 device reaches its ruggedized design limitations (e.g., maximum impact or high temperature
2027 limit). This should provide ample time to switch to another communications method or at least
2028 inform others of the failure before it occurs.
2029

2030 **8.2 Ease of Management**

2031 Certain conditions could require immediate updates to devices in a PAN. Currently, LMR keying
2032 and channel settings can require a radio to be taken out of commission, plugged into another
2033 system, updated, and then put back into commission. This process is not conducive to public
2034 safety's immediate response needs during an emergency. Ease of management should provide a
2035 secure, reliable, and efficient way to deploy and maintain devices within an organization. To
2036 achieve this, a radio operations group should have systems and devices that support over-the-air
2037 rekeying, multiple encryption keys, and system updates.

2038 Configuration management allows cellular and radio operators to set key parameters on a device.
2039 For cellular devices, a mobility device management (MDM) solution enables an administrator to
2040 configure settings such as device timeout, pin/password, approved applications, and email.
2041

2042 **8.3 Interoperability**

2043 Public safety communications systems are currently dependent on LMRs, so mobile devices and
2044 wearables must be interoperable with LMR. According to NIST SP 1108, interoperability is
2045 defined as "the capability of two or more networks, systems, devices, applications, or

2046 components to exchange and readily use information—securely, effectively, and with little or no
2047 inconvenience to the user.”[48] Interoperability will be necessary for various aspects of public
2048 safety’s communication spectrum. These different aspects of interoperability are described
2049 below.

2050 **8.3.1 Device Configuration Interoperability**

2051 Device configuration interoperability ensures that devices that function within one public safety
2052 jurisdiction can function in a similar manner within another. This assumes that the device has the
2053 correct credentials to communicate between different jurisdictions and may require key
2054 provisioning to access a different communication interface.
2055

2056 **8.3.2 Infrastructure Interoperability**

2057 With new devices being developed every day, it would be beneficial if the devices easily
2058 integrated into the current public safety infrastructure. Interoperability between different devices
2059 and systems is important to reduce costs and allow easy integration into the public safety’s
2060 system infrastructure.
2061

2062 **8.3.3 Network Interoperability**

2063 Given the potential for multiple distinct but concurrently functioning cellular public safety
2064 networks, it is important that devices function the same regardless of what network they are
2065 using. Lack of interoperability between the networks may restrict communication capabilities
2066 and thus reduce situational awareness at an emergency incident.
2067

2068 **8.3.4 Device Platform/Application/Services Interoperability**

2069 LMRs, cellular devices, and wearables are built on different platforms and operating systems.
2070 Regardless of the baseline platform of the device, the communication between the devices should
2071 be seamless to allow the first responders to focus on the emergency incidents. Applications and
2072 services developed to aide first responders should be available for use on all device platforms.
2073

2074 **8.3.5 Security Technology Interoperability**

2075 This type of interoperability stems from the need to have security technologies capable of
2076 exchanging security information such as cryptographic keys. Current practices for exchanging
2077 security information differ somewhat from jurisdiction to jurisdiction. Desktop applications are
2078 sometimes needed to properly provision LMR devices, and when multiple jurisdictions are
2079 responding to the same incident, each jurisdiction’s management application may need to be
2080 used. These applications can be expensive and difficult to manage. Alternatively, some
2081 jurisdictions support OTAR, whereas others do not. With security technology interoperability,
2082 security-relevant information can be easily exported, digested, and exchanged.
2083

2084 **8.3.6 Data Format Interoperability**

2085 When sharing data, public safety-specific information should be provided in a common public
2086 format understandable by all systems and personnel. The information exchanged between
2087 different systems should be capable of receipt and interpretation.
2088

2089 **8.4 Isolation**

2090 Isolation is the ability to keep data components and processes separate from one another. In
2091 particular, it is the ability to restrict the flow of information from one entity to another. Modern
2092 mobile devices provide varying levels of isolation, and this capability may not be present at all in
2093 many wearables.
2094

2095 **8.4.1 Data Isolation**

2096 Multiple public safety personnel stated that personal and public safety information needed to be
2097 kept separate. One common way of doing this on a mobile device is through the use of a “secure
2098 container.” Wearables often lack the ability to separate data, but wearables are often single-
2099 purpose, dedicated, embedded devices that do not contain data from multiple services, although
2100 this may change in the future.
2101

2102 **8.4.2 Application Isolation**

2103 Application isolation keeps one application from interacting with another unless it is an intended
2104 interaction. This helps keep devices running in a secure state and can prevent application exploits
2105 from being successful or at least limit their impact.
2106

2107 **8.5 Confidentiality**

2108 Confidentiality means “preserving authorized restrictions on information access and disclosure,
2109 including means for protecting personal privacy and proprietary information” [10].
2110 Confidentiality protection often occurs via access controls and data encryption. Encryption of
2111 public safety data, both in transit and at rest, did not have the same priority for every public
2112 safety discipline. For example, members of the fire service consistently identified the need for
2113 availability over data confidentiality. Law enforcement and the EMS needed data confidentiality
2114 under certain scenarios.

2115 Interviews with public safety professionals showed that encrypted connections are not used in
2116 every public safety discipline. While confidentiality protection may provide security benefits, it
2117 also contains drawbacks. Setting up secure connections may be a complex technical process with
2118 significant network bandwidth, usability, and interoperability barriers. This supports the “ease of
2119 management” objective.
2120

2121 **8.5.1 Data in Transit**

2122 Data in transit refers to protecting data transmitted over a network connection, such as protecting
2123 a patient’s information as it is transmitted from an EMT’s radio to a hospital. Another example is
2124 ensuring that a Bluetooth throat microphone is securely communicating with a mobile device.
2125

2126 **8.5.2 Data at Rest**

2127 Data at rest refers to protecting data stored on a device, such as encrypting pictures of a crime
2128 scene taken by a police officer or patient data encrypted on a mobile device during transport in
2129 an ambulance.

2130 **8.6 Authentication**

2131 NISTIR 7298, *Glossary of Key Information Security Terms* defines authentication as “verifying
2132 the identity of a user, process, or device, often as a prerequisite to allowing access to resources in
2133 an information system” [10]. Authentication is necessary to ensure that only authorized public
2134 safety users have access to public safety resources. Below are types of authentications that are
2135 applicable to public safety.
2136

2137 **8.6.1 Ease of Authentication**

2138 First responders need to have an efficient way of authenticating to their device(s) in emergency
2139 situations. Complicated passwords and authentication tokens can interfere with the first
2140 responder’s focus on the mission. Multiple authentication methods exist and should be analyzed
2141 for use. NISTIR 8080 *Usability and Security Considerations for Public Safety Mobile*
2142 *Authentication* discusses this and other usability issues first responders face as well as how they
2143 impact other areas of security [11].
2144

2145 **8.6.2 User to Device Authentication**

2146 In many instances, especially law enforcement, it is important to prevent external entities from
2147 accessing information stored on a lost or stolen device. User to device authentication does not
2148 prevent sensitive information from appearing on the lockscreen via notifications. Notifications to
2149 a locked device are available to anyone who has physical access to the device.
2150

2151 **8.6.3 Device to Network Authentication**

2152 During large-scale emergency events, telecommunication networks tend to become extremely
2153 congested. Priority and preemption for public safety users is necessary to ensure that they can
2154 communicate with each other, and proper authentication ensures successful implementation. In
2155 addition, there is the simple requirement of ensuring that unauthorized devices are not allowed to
2156 access the network.
2157

2158 **8.6.4 User to Third-party Service, Wearable, or Device Authentication**

2159 Users may also need to authenticate to individual applications, wearables, and third-party
2160 services. This authentication provides another layer of security to a first responder’s device and
2161 applications. If a device is compromised, an unauthorized user would not be able to access public
2162 safety information on applications or devices due to strong authentication requirements.
2163

2164 **8.7 Integrity**

2165 Integrity guards against improper data modification or destruction and includes ensuring
2166 information non-repudiation and authenticity [10]. Mobile devices must protect against
2167 corruption in hardware, firmware, and software. A rooted or “jailbroken” device bypasses system
2168 integrity checks, allowing the underlying OS and firmware to be manipulated—possibly
2169 unbeknownst to the user. This poses a significant risk to data and voice communications and
2170 applications used to access agency assets. Device manufactures can strengthen their validation
2171 methods by deploying a hardware root of trust (e.g., secure enclave, secure element).

2172 Device manufacturers can customize the low-level OS and boot functions through a boot ROM
2173 agent that validates the boot loader and OS. This boot ROM agent acts as an additional root of
2174 trust and is critical to ensuring the operating system and firmware have not been tampered with.

2175

2176 **8.8 Device and Ecosystem Health**

2177 **8.8.1 Configurations**

2178 Public safety mobile devices may be customized for first responder’s operational needs.
2179 Customized device operating systems can significantly vary in versions that ship with standard
2180 commercial devices. Large portions of the OS may be missing, modified, or replaced. Public
2181 safety device OEMs may also add new features unique to public safety to the OS, which may not
2182 receive the same level of security assessment as when implemented on large-scale deployment
2183 commercial devices. Due in part to these changes to the mobile OS, default security
2184 configurations and settings may not be configured in the same way as traditional COTS devices.
2185 This includes device encryption, pre-installed applications, authentication options, and other
2186 configuration options. While these configurations may assist in deployment to the field and be
2187 useful to public safety, minor misconfigurations can greatly affect the overall security of the
2188 device.

2189 **8.8.2 Updates**

2190 Over time, software, firmware, and hardware vulnerabilities are commonly identified in any
2191 information system. These issues may be exploitable by an adversarial threat source, leaving
2192 public safety devices vulnerable to many forms of security exploits. Closing these holes is most
2193 often performed by software updates and the security patching process. Yet many distinct
2194 organizations work in concert to supply the hardware and software components of smartphones
2195 and wearables, making the update process cumbersome. For instance, any device with a cellular

2196 radio has additional parties in this supply chain such as cellular carriers and baseband chipset
2197 designers.

2198 It is difficult for many distinct entities to work together to develop, test, and deploy patches to
2199 such diverse systems, and it is challenging to coordinate between those entities to provide timely
2200 and effective updates that do not disrupt the functionality of the device. As such, a patch for the
2201 operating system could take a few months to over a year to reach the end-users' device. A device
2202 hardware manufacturer may also opt to delay updates in order to preserve the stability of device
2203 and application functionality. Users may need to weigh the risk of delayed security patches
2204 against device stability for their operations.

2205 **8.8.3 Bundled Applications**

2206 As previously mentioned, first responder applications are often preinstalled on public safety
2207 mobile devices. These applications provide functionality like PTT, computer aided dispatch
2208 (CAD) alerts, and local event notifications. Mobile applications receive some security review
2209 through the third-party application store (e.g., Apple App Store, Google Play, and the new
2210 FirstNet App Developer Program) before they are posted. A device manufacturer can also install
2211 applications onto a device through their own app store or by side-loading (i.e., manually
2212 installing). Regardless of installation origin, these applications should be vetted, monitored, and
2213 updated in a timely manner.

2214 9 Conclusions

2215 This study performed foundational research at the intersection of cybersecurity and public safety
2216 communications, and it helps to form the foundation for how to ensure the security and reliability
2217 of public safety communications. Relevant public safety use cases for mobile devices and
2218 wearables were identified, and the cybersecurity considerations for use cases were analyzed.
2219 Previous attacks on public safety systems were described, informing a threat analysis to analyze
2220 how potential security issues may affect public safety agencies. Finally, the information gleaned
2221 from this study was used in conjunction with information collected directly from interviews with
2222 public safety professionals to define security objectives for mobile devices and wearables.

2223 Public safety has an inherent need for availability of telecommunications systems whereas
2224 confidentiality and integrity are sometimes considered secondary and tertiary needs. The results
2225 of this study support the notion that mobile devices, tablets, and wearables used by public safety
2226 have a very strong need for availability. Yet a more nuanced view is necessary, as confidentiality
2227 and integrity must also be thoroughly evaluated within each public safety discipline. For
2228 instance, the fire service requires high availability, whereas law enforcement and the EMS have
2229 regulatory considerations for data confidentiality (e.g., HIPAA). Depending on the emergency
2230 situation, the fire service may also require data confidentiality if the firefighter is handling
2231 patient information. That said, the type of emergency incident also contributes to the evaluation
2232 of the necessary security objectives for each public safety discipline.

2233 A major conclusion of this effort is the need to develop robust and innovative mitigations for the
2234 threats identified within this report, along with practical guidance for their implementation. The
2235 transition from LMR to cellular technologies will take time but will also introduce a plethora of
2236 new technologies. Technologies like EMM to manage devices, mobile threat defense for
2237 endpoint protection, application vetting to ensure apps are safe and free of vulnerabilities, and
2238 encryption to prevent eavesdropping are all necessary to protect public safety communications.
2239 All of these are sufficiently complex, requiring an experienced professional to implement and
2240 properly configure them.

2241 Little guidance exists for the appropriate configurations for public safety devices, let alone
2242 configurations for specific disciplines. These new technologies have a strong potential to
2243 introduce new vulnerabilities into a jurisdiction's network. Therefore, it is important for this
2244 class of devices to be scrutinized in a manner similar to COTS devices or perhaps even more so
2245 given the sensitivity of public safety data. Yet to date, there are few examples of such a security
2246 analysis from academic, government, or industry security professionals.

2247 Under PSCR's security portfolio, there is authentication research with regards to mobile single
2248 sign-on (SSO) [59]. This research analyzes how mobile SSO can be implemented on a mobile
2249 device and used by first responders to authenticate once and gain access to multiple services on
2250 their devices. This research analyzes ease of authentication requirements, improving
2251 authentication assurance, and federating identities and user account management.

2252 Within PSCR's mission critical voice (MCV) portfolio, there is research into the availability
2253 concerns for first responders. The research considers in-building communication coverage.

2254 More specifically, the research identifies ways to assess the in-building measurement and
2255 coverage quality of LTE. This research will provide first responders with awareness of LTE
2256 coverage within assessed buildings and ultimately improve coverage in such areas.

2257 It is critical that the transition of public safety communications systems and devices to next
2258 generation technology occur in a smooth manner. By understanding the threats and risks posed to
2259 public safety systems and their users, life-threatening scenarios can be prevented from escalating
2260 due to malicious or accidental failures of technology. The following topics are open research
2261 areas in this space:

- 2262 • Prevention of public safety device and user tracking
- 2263 • Discipline-specific EMM policy configurations
- 2264 • Low cost ways to implement EMM and mobile supporting technology
- 2265 • Mitigations for protocol-jamming attacks that do not require redesigns of public safety
2266 devices
- 2267 • Methods to add confidentiality and integrity protection to low cost wearables that
2268 insecurely transmit public safety information
- 2269 • Best practices for updating the software on mobile devices and wearables
- 2270 • Device lockscreen timeout recommendations
- 2271 • Authentication mechanisms that have high assurance but are simple and non-intrusive
- 2272 • Operational guidance for device sharing
- 2273 • Ruggedizing mobile devices and wearables to public safety needs

2274 For more information on this and other NIST security and public safety communications
2275 projects, please visit <https://www.nist.gov/ctl/pscr/newsroom>.

2276 **Appendix A—Acronyms**

2277 Selected acronyms and abbreviations used in this paper are defined below.

2278	2G	2 nd Generation
2279	3G	3 rd Generation
2280	3GPP	3 rd Generation Partnership Project
2281	4G	4 th Generation
2282	5G	5 th Generation
2283	APCO	Association of Public Safety Communications Officials
2284	BYOD	Bring Your Own Device
2285	CAD	Computer-aided Dispatch
2286	CERT	Computer Emergency Response Team
2287	COTS	Commercial Off-The-Shelf
2288	DC	District of Columbia
2289	DHS	Department of Homeland Security
2290	EMM	Enterprise Mobility Management
2291	EMS	Emergency Medical Services
2292	EMT	Emergency Medical Technician
2293	EPCR	Electronic Patient Care Reporting
2294	FHSS	Frequency Hopping Spread Spectrum
2295	FM	Frequency Modulation
2296	GhZ	Gigahertz
2297	GPS	Global Positioning System
2298	GSM	Global System for Mobile Communications
2299	IEEE	Institute of Electrical and Electronics Engineers
2300	IR	Interagency Report
2301	IoT	Internet of Things
2302	ISM	Industrial, scientific and medical
2303	ISO	International Organization for Standardization
2304	ITL	Information Technology Laboratory
2305	KBA	Knowledge-based authentication
2306	LE	Low Energy
2307	LEO	Law Enforcement Officer
2308	LMR	Land Mobile Radio
2309	LTE	Long Term Evolution
2310	MCI	Mass Casualty Incident
2311	MCV	Mission Critical Voice
2312	MDT	Mobile Data Terminal
2313	MFA	Multifactor Authentication
2314	MHz	Megahertz
2315	NCIC	National Crime Information Center
2316	NFC	Near Field Communication
2317	NFPA	National Fire Protection Association
2318	NIST	National Institute of Standards and Technology
2319	NPPD	National Protection Programs Directorate

2320	NPSBN	Nationwide Public Safety Broadband Network
2321	NPSTC	National Public Safety Telecommunications Council
2322	OS	Operating System
2323	OTP	One-Time Password
2324	P25	Project 25
2325	PAN	Personal Area Network
2326	PII	Personally Identifiable Information
2327	PIN	Personal Identification Number
2328	PIV	Personal Identity Verification
2329	PKI	Public Key Infrastructure
2330	PPE	Personal Protective Equipment
2331	PSAC	Public Safety Advisory Committee
2332	PSCR	Public Safety Communications Research
2333	PTT	Push-To-Talk
2334	RFID	Radio-Frequency Identification
2335	SCBA	Self-Contained Breathing Apparatus
2336	SIM	Subscriber Identity Module
2337	SME	Subject Matter Expert
2338	SoR	Statement of Requirements
2339	SP	Special Publication
2340	SSO	Single Sign-on
2341	TLS	Transport Layer Security
2342	UI	User Interface
2343	UICC	Universal Integrated Circuit Card
2344	UHF	Ultra High Frequency
2345	UMTS	Universal Mobile Telecommunications System
2346	USB	Universal Serial Bus
2347	VDI	Virtual Desktop Infrastructure
2348	VHF	Very High Frequency
2349	VPN	Virtual Private Network
2350		

2351

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, *Assessing 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 Firmware 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] Padgett 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 Institute 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](http://www.firstnet.gov/sites/default/files/PSAC%20Use%20Cases%20Report.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-conflicker-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] Rugar, 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 911 emergency 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, December 2014. <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 Stakeholder 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>.