Office of Emergency Communications:

Cyber Risks to Next Generation 9-1-1

November 2018

SAFECOM™ NCSWIC™ Homeland Security

Cyber Risks to Next Generation 9-1-1

Next Generation 9-1-1 (NG9-1-1) systems, which operate on an Internet Protocol (IP) platform, enable interconnection among a wide range of public and private networks, such as wireless networks, the Internet, and regular phone networks. NG9-1-1 systems will enhance the capabilities of today's 9-1-1 networks, allowing compatibility with more types of communication, providing greater situational awareness to dispatchers and emergency responders, and establishing a level of resiliency not previously possible. NG9-1-1 will allow Public Safety Answering Points (PSAPs) to accept and process a range of information from responders and the public, including text, images, video, and voice calls.

How to Use this Document

This document provides an introduction to:

- Next Generation 9-1-1 (NG9-1-1) systems
- The NG9-1-1 cybersecurity risk landscape
- Resources to improve cybersecurity posture

Public safety managers and officials can use this document to familiarize themselves with NG9-1-1 systems and best practices to maintain and improve cybersecurity posture. This document provides sample risk reduction strategies, actions, and resources. It does not contain specific, system-unique instructions or address governance considerations.

Traditional 9-1-1 services typically operate over standard voice-based telephone networks and use software, such as computer-aided dispatch systems, that operate on closed, internal networks with little to no interconnection with other systems. The relatively limited means of entry into legacy 9-1-1 systems reduces the potential attack vectors. However, cyber risk is still a concern and must be actively managed, even with legacy systems. NG9-1-1 interconnections enable new benefits, as shown in Figure 1. However, they also represent new vectors for attack that can disrupt or disable PSAP operations, broadening the concerns of—and complicating the mitigation and management of—cyber risks across all levels of government.

Potential cyber risks to NG9-1-1 systems do not undermine the benefits of NG9-1-1. Nevertheless, cyber risks present a new level of exposure that PSAP administrators must understand and actively manage as a part of a comprehensive risk management program. Systems are already under attack. As cyber threats grow in complexity and sophistication, attacks could be more severe against NG9-1-1 systems as attackers can launch multiple distributed attacks with greater automation from a broader geography and against more targets. This document provides an overview of the cyber risk landscape, offers an approach for assessing and managing risk, and provides additional cybersecurity resources.

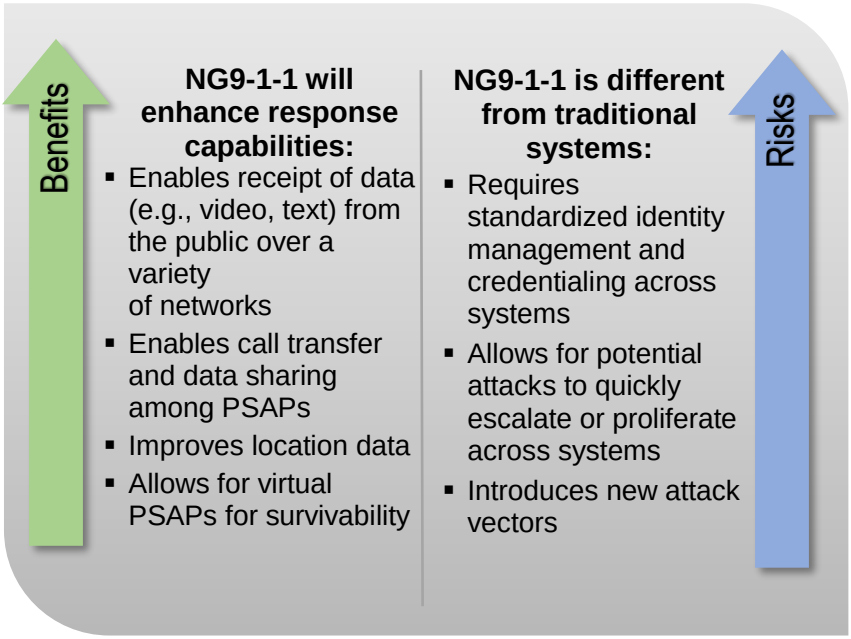

Figure 1. NG9-1-1 Benefits and Risks

NG9-1-1 Cybersecurity Risk Landscape

Cybersecurity[1] risks occur when a *threat* exploits a *vulnerability*, leading to an undesired event that has a negative *consequence* on the desired state of the network. The terms that define risk—*threat*, *vulnerability*, *likelihood,* and *consequence*—are further described in Appendix C. Cybersecurity risks to NG9-1-1 systems, such as those shown in Figure 2, have severe potential impacts, including loss of life or property; job disruption for affected network users; and financial costs from the misuse of data and subsequent resolution. Appendix D contains examples of real-world public safety and 9-1-1 cyber attacks.

User and Devices	Network Infrastructure and Connections	Data, Applications and Services
• **Data breaches**: Data on device is accessed, manipulated, or stolen • **Insider threats**: Employees or other authorized personnel steal, corrupt, or destroy data • **Malware**: Download of malicious software (e.g., botnets, viruses, spyware, Trojans, rootkits) • **Ransomware**: Use of software to block computer systems for the purpose of extorting a ransom • **Spear-phishing**: Targeted social engineering attacks enable criminals to access sensitive data • **Spoofing**: Unauthorized device masquerades as an authorized device	• **Denial-of-service attack**: Attackers overload network resources with requests for access, straining the operability and capacity of the network; or use RF Jamming techniques to prevent wireless, cellular, broadband, or land mobile radio (LMR) communications. • **Man-in-the-middle attack**: Wireless link between the user device and the tower may be susceptible and allow attackers to steal data or monitor conversations • **Telephony-Denial-of-service-attack**: Use of Voice over Internet Protocol systems to overwhelm the PSAP's phone system, rendering the center incapable of placing or receiving calls • **Unauthorized network access**: Bypass of authorized methods and procedures	• **Malicious applications**: Attackers create apps that appear to be safe but allow them to steal, corrupt, or modify data, eavesdrop on conversations, or acquire data on the location of victims and/or first responders • **Swatting**: Manipulation of IP-based 911 calls to indicate the call is originating from a location at which a most serious criminal act has taken or is taking place, prompting local PSAP to dispatch a Special Weapons and Tactics (SWAT) team to the address • **Unauthorized data access**: Attackers can access sensitive databases (e.g., law enforcement, health records) to steal, modify, or corrupt the data
Consequences: Any of the risks above can impact communications and operations in a negative manner and disrupt: • Confidentiality—*Ensures that data is only accessed by those authorized to see it;* • Integrity—*Ensures that data is trustworthy and is not altered through transmittal, storage, or retrieval, and/or;* • Availability—*Ensures that the infrastructure is operational and committable to its intended purpose*.		

Figure 2. Potential Risks to NG9-1-1 System Components

Cyber infrastructure[2] for NG9-1-1 systems that must be protected includes networks, assets, databases, and services involved in the processing, storage, and transport of data. Specifically, an NG9-1-1 system's cyber infrastructure includes:

- Assets that are part of, or interconnect with, Emergency Services IP Networks (ESInets)
- Service provider networks and applications that interconnect with ESInets
- Government applications and services that connect to ESInets
- Dispatch systems and components that connect to ESInets

Appendix B further describes NG9-1-1 cyber infrastructure. Traditionally, the term "cyber" has been applied to only information technology (IT) systems and assets, while communications infrastructure was considered separate. However, defining cyber infrastructure as including both IT and communications systems accounts for the many ways in which these systems have converged. 9-1-1 authorities and agencies must recognize this convergence to more effectively counter risks. Risks to any component of these systems could threaten a NG9-1-1 system, its data, and any *interconnected* system. It is imperative to consider security holistically.

[1] Cybersecurity is "the prevention of damage to, unauthorized use of, exploitation of, and, if needed, the restoration of electronic information and communications systems and services (and the information contained therein) to ensure confidentiality, integrity, and availability", Department of Homeland Security (DHS) National Infrastructure Protection Plan (NIPP), 2009. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[2] "Cyber infrastructure includes electronic information and communication systems, and the information contained in these systems…Information and communications systems are composed of hardware and software that process, store, and communicate data of all types. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information." DHS NIPP, 2009. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

Improving NG9-1-1 Cybersecurity Posture

Given the dynamic nature of technology and the evolving cyber risk landscape, organizations should adopt a cybersecurity risk management process. An effective process enables response organizations to:

- Identify new and evolving risks
- Assess and prioritize risks
- Develop and prioritize mitigation strategies based on cost-benefit analysis and other factors
- Evaluate the impacts of mitigation implementation
- Develop an approach to detection and effective response and recovery procedures

The Department of Homeland Security (DHS) strongly recommends implementing the NIST Cybersecurity Framework, which is a flexible, risk-based approach to improving the security of critical infrastructure.[3] Collaboratively developed between government and the private sector, the framework is designed to complement an existing risk management process or to develop a credible program if one does not exist.[4]

Identifying and Assessing Risks

Regardless of the cybersecurity risk management process implemented, administrators will need to identify, evaluate, and prioritize risks for their organization. Figure 3 provides a sample risk assessment process.

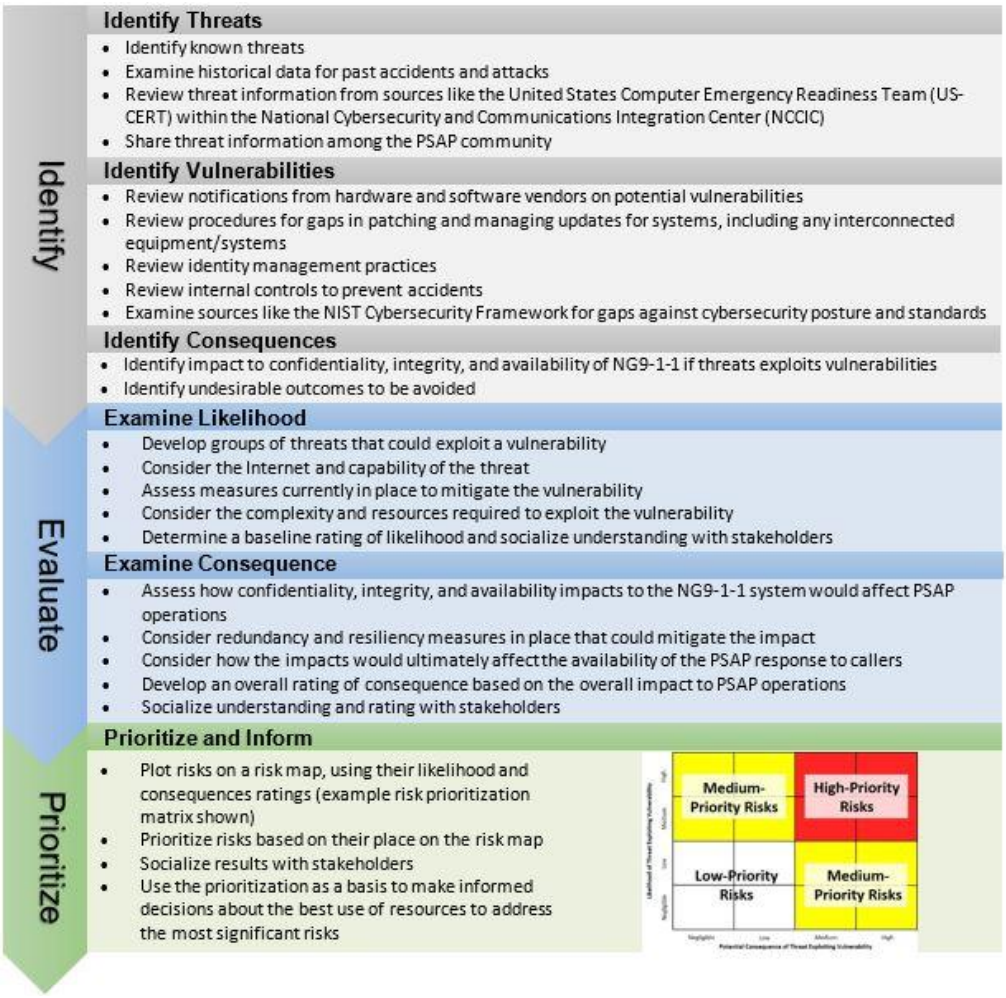

Figure 3. Sample Risk Assessment Plan (to be followed with mitigation and response/recovery)

[3] The most recent NIST Cybersecurity Framework and related newsletters are available at http://www.nist.gov/cyberframework/.
[4] Ibid.

Mitigating Risks: Protect and Detect

While no single mitigation strategy can comprehensively address all risk scenarios, individual evaluation of mitigation techniques may identify complementary strategies for the creation of a broad-reaching, holistic approach. In general, mitigation techniques aim to either prevent and protect against an identified threat, or seek to ensure timely awareness of a cybersecurity breach. Mitigation strategies should employ safeguards that decrease the consequence of a risk, if exploited, on the ability to deliver critical services.

Table 1 describes sample mitigation strategies for NG9-1-1. This list is not exhaustive and should not replace a comprehensive requirements analysis; it is simply intended to enhance planning discussions. Some elements may be addressed through standards, industry best practices, or policy guidance, while others may be developed by PSAP administrators.

Table 1. Sample NG9-1-1 Security Mitigation Strategies (Non-Comprehensive)

SAMPLE Strategy		Description
Protect	Access Privileges	Ensure access privileges are used appropriately and that privilege elevations are restricted to appropriate personnel
	Application Layer Interoperability	Determine application layer interoperability requirements and standards and implement a process for regular review and update
	Authentication and Identity Management	Develop and implement policies on authentication and identity management that are applied uniformly and meet public safety requirements for performance, security, and time-sensitive mission demands
	Capacity Planning	Engage in assessing capacity requirements for PSAP infrastructure and assets
	Data Encryption	Develop requirements for data encryption that apply to both primary and back-up data
	Database Back-Up	Develop guidance or policies for performing and retrieving database backups
	Information Security Policies	Establish and enforce consistent information security policies and ensure those policies are continually updated as new threats and technologies emerge
	Training	Develop role-specific training requirements for users and administrators, to include training on security, resiliency, and operations
Detect	Continuous Monitoring	Develop continuous diagnostics and mitigation capabilities or use existing government capabilities
	Log Management and Audit Capabilities	Ensure that log management and audit capabilities, policies, and technology are strong, appropriate, and responsive
	Physical Security and Access Control	Develop and implement physical security and access control policies for facilities

Exploited Risks: Response and Recovery

Incident Response Teams (IRT), incident response plans, recovery or resiliency plans, and continuity of operations plans are useful in cybersecurity incident response. PSAP administrators may consider establishing a Computer Security Incident Response Team (CSIRT) or reach an agreement with US-CERT, run by the DHS National Cybersecurity and Communications Integration Center (NCCIC), to assist in carrying out cybersecurity planning.[5] A CSIRT serves as a centralized location to report and analyze security issues within an organization. A CSIRT may also recommend potential solutions to threats and publicize known threats, vulnerabilities, and solutions generally or to a specific information-sharing community. The CSIRT can work with hardware and software vendors to obtain information about vulnerabilities and potential solutions. Leveraging federal resources, such as US-CERT, can aid in the protection of NG9-1-1 systems. Also, coordinating response and recovery efforts with the Statewide Interoperability Coordinator (SWIC), State Single Points of Contact (SPOC), and other PSAP administrators can increase cybersecurity posture. Table 2 shows sample response and recovery actions.

Table 2. Sample NG9-1-1 Response and Recovery Actions (Non-Comprehensive)

SAMPLE Action	Description
Response	▪ **Incident Response Plan.** Develop incident response plans, policies, and capabilities for the networks, personnel, and user equipment that prevent expansion of the event, mitigate its effects, and eradicate the incident ▪ **Incident Response Team (IRT).** Establish an incident response team or utilize existing capabilities like US-CERT to ensure response activities are coordinated with appropriate stakeholders ▪ **Contain Cybersecurity Event.** Execute response processes and procedures, preventing expansion of the event, mitigate its effects, and eradicate the incident ▪ **Deploy IRT.** Coordinate with internal and external stakeholders, as appropriate, including external support from law enforcement agencies and response centers, such as US-CERT
Recovery	▪ **Recovery Plan.** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event ▪ **Continuity Planning.**[6] Establishing and maintaining redundancy is a key strategy that promotes network reliability, resiliency, and continuity of service ▪ **Coordination.** Restoration activities are coordinated with internal and external parties, such as coordinating centers, internet service providers, owners of attacking systems, victims, response partners, and vendors ▪ **Process Improvements.** Recovery planning processes and strategies are improved by incorporating lessons learned into future activities. Response personnel should be trained on the latest security, resiliency, continuity and operational practices and maintain in-service training as new technology and methods are made available

Once risks are identified and protective mitigations are in place, the NG9-1-1 community has an opportunity to focus on detection and advanced planning. Instead of focusing on individual cybersecurity events and data recovery, a mature cybersecurity risk management plan uses data analytics in PSAPs, joint field offices, emergency operations centers, fusion centers, and other cyber centers to accelerate and automate analysis.

[5] See: https://www.us-cert.gov/ccubedvp.

[6] For continuity recommendations, see FEMA's Continuity Guidance Circular (CGC) available at https://www.fema.gov/continuity-guidance-circular-cgc.

Actions for Improving NG9-1-1 Cybersecurity

This document provides an overview of the cyber risks impacting NG9-1-1 systems. It is intended to serve only as an informational tool for public safety system administrators and officials to better understand the full scope and range of potential risks, as well as recommend mitigations to these risks. The following actions are recommended for system administrators and officials to improve their NG9-1-1 systems:

Adopt a "security first" perspective. Cybersecurity has become an integral part of mission function and operations for NG9-1-1 systems. **Cyber defense should be at the forefront of NG9-1-1 planning, as opposed to an afterthought.** Working with others within the NG9-1-1 community, government, industry, and academia to establish consistent security guidance for NG9-1-1 deployments is crucial.

- **Leverage historically-successful cybersecurity strategies.** Researching available references and resources, as well as gathering experiences from other NG9-1-1 community members, is important to constructing the ideal solution set for each NG9-1-1 system's unique circumstances.
- **Establish a CSIRT or reach an agreement with US-CERT to assist in carrying out cybersecurity planning.** A CSIRT serves as a centralized location to report, analyze, and respond to security issues. CSIRTs also track developments in the field and provide prioritized implementation of cyber solutions.
- **Establish a cybersecurity risk framework.** The NIST Cybersecurity Framework is highly recommended as a flexible, risk-based approach to improving the security of critical infrastructure.
- **Identify, evaluate, and prioritize risks using a community-based risk assessment process.** To identify and assess vulnerabilities in their own systems, PSAP administrators should work closely with all partners with whom they interconnect, such as service providers, neighboring jurisdictions, and other agencies to identify the full architecture of their system and assess it for physical and network vulnerabilities. This assessment should include a review of their processes and standard operating procedures against government and industry cybersecurity best practices and standards.
- **Develop relationships to strengthen cybersecurity posture.** Establishing and maintaining relationships to develop and execute a comprehensive cybersecurity plan could involve sharing resources among multiple PSAPS, and/or among multiple local, regional, or state agencies with the necessary expertise and resources.
- **Implement mitigations.** An examination of the likelihood and consequences of attacks should help to prioritize and inform mitigation strategies. Using both prevention and detection techniques, administrators should strive to negate or decrease the impact of an attack. Researching mitigation techniques and employing them in a prioritized fashion will improve cybersecurity posture.
- **Solidify Response and Recovery actions.** Establishing a CSIRT and developing incident response plans, policies, and capabilities for the network, personnel, and user equipment can prevent expansion of the event, mitigate its effects, and eradicate the incident. These efforts should be supported by regular training and exercises and coordination with external parties so that all participants are aware and capable of their role during and after an event.

Appendix A provides additional educational, operational, and training resources for NG9-1-1 cybersecurity. The resources provided are not exhaustive and do not imply endorsement for organizations or their products. As cyber threats grow in complexity and sophistication, attacks could be more severe against NG9-1-1 systems as attackers can launch multiple distributed attacks with greater automation, from a broader geography, and against more targets. It is imperative that the NG9-1-1 community remain engaged in cybersecurity risk management and actively maintain an enhanced cybersecurity posture for their systems.

Appendix A: Next Generation 9-1-1 Cybersecurity Resources

Tables A-1, A-2, and A-3 provide non-comprehensive lists of available resources for NG9-1-1 administrators to learn more and improve the cybersecurity posture of their systems. **The resources provided are not exhaustive and do not imply endorsement for organizations or their products.**

Table A-1. Government NG9-1-1 Resources

Organization	Resource Name	Description and Link
Department of Homeland Security (DHS)	Office of Emergency Communications	DHS offers a collection of programs and initiatives that can be applied to reduce NG9-1-1 cyber risks. Many of these efforts support approved missions that cover federal, state, and local users, as well as public and private critical infrastructure entities. https://www.dhs.gov/office-emergency-communications
	National Cybersecurity and Communications Integration Center (NCCIC)	NCCIC is a 24/7 cyber monitoring, incident response, and management center. Organizations can leverage NCCIC's United States Computer Emergency Readiness Team (US-CERT) for cybersecurity information and assistance. https://www.dhs.gov/national-cybersecurity-and-communications-integration-center
Federal Communications Commissions (FCC)	Legal and Regulatory Framework for NG9-1-1 Services	An overview on the development and creation of a NG9-1-1 network that provides specific citations from the FCC on statutory requirements and funding possibilities. https://apps.fcc.gov/edocs_public/attachmatch/DOC-319165A1.pdf
	Communications Security, Reliability and Interoperability Council (CSRIC)	CSRIC's mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety. Guidance includes: • Transition to Next Generation 9-1-1. https://transition.fcc.gov/pshs/docs/csric/CSRIC-WG4B-Final-Report.pdf • Cybersecurity Risk Management and Best Practices. https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf
	Task Force on Optimal PSAP Architecture (TFOPA): Optimal Cybersecurity Approach for PSAPs	The TFOPA provided recommendations to the FCC regarding actions that PSAPs can take to optimize their security, operations, and funding as they migrate to NG9-1-1, including the establishment of Emergency Communications Cybersecurity Centers (EC3s). https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG1_FINAL_Report-121015.pdf
	Blog	For example, this FCC blog entry focuses on how PSAPs can create a culture of and boost cybersecurity. Other pertinent resources are also linked in the entry. https://www.fcc.gov/news-events/blog/2016/01/28/creating-culture-cybersecurity-america%E2%80%99s-9-1-1-call-centers
National 9-1-1 Program	911.gov	911.gov is a comprehensive resource for all things related to NG9-1-1. The website includes resources related to technical 9-1-1 issues and policy, NG9-1-1 related standards, and a 9-1-1 profile database for tracking the progress of 9-1-1 authorities across the nation. https:/www.911.gov In addition, 911.gov hosts a comprehensive collection of cybersecurity documents and resources. https://www.911.gov/issue_cybersecurity.html
National Institute of Standards and Technology (NIST)	Cybersecurity Framework	The NIST Cybersecurity Framework is a prioritized, flexible, repeatable, and cost-effective approach that can help NG9-1-1 system administrators manage cybersecurity-related risks. https://www.nist.gov/cyberframework
	Baldrige Cybersecurity Excellence Builder	This is a cybersecurity framework self-assessment tool PSAPs can use to better understand the effectiveness of their cybersecurity efforts. https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative
	National Initiative for Cybersecurity Education (NICE)	NICE provides an additional cybersecurity framework for PSAPs. This framework describes cybersecurity by categories, specialty areas, work roles, knowledge, skills, and abilities. https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework
	Recommendations on Cybersecurity (Special Publications 800/1800 Series)	NIST's 800 and 1800 series provides targeted cybersecurity guidance and are strongly encouraged to be incorporated into cybersecurity planning. https://csrc.nist.gov/publications/sp#SP800

Table A-2. Industry and Trade Association Cybersecurity Resources

Organization	Description and Link
Association of Public-Safety Communications Officials-International (APCO)	APCO has sections dedicated to cybersecurity, as well as other helpful materials on its website: https://www.apcointl.org/advocacy/topics/cybersecurity.html • "An Introduction to Cybersecurity" https://www.apcointl.org/download/introduction-to-cyber-security-a-guide-for-psaps/?wpdmdl=6250
Alliance for Telecommunications Industry Solutions (ATIS)	ATIS provides public safety industry best practices ranging from "important," "highly important," to "critical" for PSAPs. http://www.atis.org/bestpractices/Search.aspx
Center for Internet Security (CIS)	CIS gives cybersecurity tips and warnings on recently discovered vulnerabilities and threats. https://www.cisecurity.org/resources/
Government Technology	Government Technology magazine reports the latest on public sector information technology. There is a section dedicated to NG9-1-1 on its website. http://www.govtech.com/em/next-gen-9-1-1/
ISACA	ISACA develops best practices for information systems. Their COBIT 5 framework provides IT governance and management practices. http://www.isaca.org/cobit/
International Telecommunications Union (ITU)	PSAPs can utilize ITU's Security Standards Roadmap to develop security standards and gain understanding of existing standards and those that are in progress. http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/default.aspx
National Emergency Number Association (NENA)	NENA's website contains a complete archive of all its 9-1-1 standards, including those related to NG9-1-1, such as the i3 suite of standards and the NG-SEC standard (NENA 75-001). https://www.nena.org/?page=Standards
Open Web Application Security Project (OWASP)	OWASP is an online community that focuses on web application security. The website hosts free security-related resources. https://www.owasp.org/index.php/Main_Page
SANS Institute	SANS Institute's 20 Critical Security Controls details prioritized cyber defense actions that can help PSAPs prevent and mitigate cyber risks. https://www.sans.org/critical-security-controls
SecuLore Solutions	SecuLore offers public safety-oriented cybersecurity products and services. Its resource webpage archives cyber attacks, cyber guidelines, and webinars. https://www.seculore.com/resources
Urgent Communications	Urgent Communications provides news and publications on information and communication technology. There is a section dedicated to NG9-1-1 on its website. http://urgentcomm.com/topics/ng-9-1-1

Table A-3. Cybersecurity Training Resources

Organization	Description and Link
APCO Envision	APCO Envision hosts intensive training on cybersecurity and NG9-1-1 for emergency communications professionals. https://www.apcoenvision.org/
Center for Development of Security Excellence (CDSE)	The Security Awareness Hub from CDSE offers free cybersecurity training that raises overall cybersecurity awareness and knowledge. https://securityawareness.usalearning.gov/index.html
Cofense	Cofense offers 17 free interactive cybersecurity training modules upon registration with the website. https://cofense.com/resources/cbfree-computer-based-training/
Cybrary	Cybrary is an online learning platform that offers free courses on cybersecurity, IT, and related fields. https://www.cybrary.it/
FireEye	Security company FireEye presents reports, training, whitepapers, and other cybersecurity resources to the public. https://www.fireeye.com/current-threats.html
Information Assurance Support Environment	DISA also offers free cybersecurity training on different topics to strengthen cybersecurity awareness. https://iase.disa.mil/eta/Pages/index.aspx

InfoSec Institute Security IQ	InfoSec Institute offers enterprise cybersecurity lessons and training both free and paid via Security IQ. https://securityiq.infosecinstitute.com/
ISACA Cybersecurity Nexus	ISACA Cybersecurity Nexus is another site that offers enterprise cybersecurity training. https://cybersecurity.isaca.org/
National Association of State Chief Information Officers (NASCIO)	NASCIO provides cybersecurity awareness resources for states including best practices and the NASCIO Cyber Disruption Response Planning Guide • https://www.nascio.org/Advocacy/Cybersecurity • https://www.nascio.org/Publications/ArtMID/485/ArticleID/358/Cyber-Disruption-Response-Planning-Guide
National Conference of State Legislatures (NCSL)	PSAPs can expand their cybersecurity training resources by incorporating information on cybersecurity training for state employees compiled by NCSL. http://www.ncsl.org/ncsl-in-dc/standing-committees/law-criminal-justice-and-public-safety/state-cybersecurity-training-for-state-employees.aspx
National Emergency Number Association (NENA)	NENA offers cybersecurity training throughout the year and at different locations. • NENA Education Calendar: http://www.nena.org/?page=educationcalendar • NENA 2018 Breakouts: https://www.nena.org/page/NENA2018Breakouts
SANS Institute Cyber Aces	SANS Institute offers online cybersecurity courses via Cyber Aces. http://www.cyberaces.org/
Secureset Academy	Secureset Academy offers intensive introductory, technical, and analytical cybersecurity training in Colorado and Florida. https://secureset.com/
Symantec	Symantec is a security company that offers courses and materials on security awareness. https://www.symantec.com/services/education-services/campaigns/security-awareness
Udemy Cybersecurity Courses	Udemy is an online learning platform that offers course on cybersecurity, IT, and related fields. https://www.udemy.com/topic/cyber-security/

Appendix B: Next Generation 9-1-1 Cyber Infrastructure

NG9-1-1 is an IP-based system designed to provide a secure, nationwide, interoperable, standards-based communications infrastructure. This will enable end-to-end transmission of all types of data, including voice and multi-media communications, from the public to an Emergency Communications Center. This approach provides much needed data and communications services to public safety in a modern, interoperable format, rather than continuing to be limited by legacy, non-interoperable implementations of 9-1-1. There are several basic building blocks of NG9-1-1 systems, as described below:

- **Emergency Services IP Networks (ESInets).** ESInets are at the center of NG9-1-1 systems. These broadband networks are engineered and managed to use Internet Protocols and standards to carry voice and data traffic (e.g., text, pictures, videos) in support of local, regional, state, and national emergency management authorities. A simplified ESInet diagram is shown in Figure B-1.

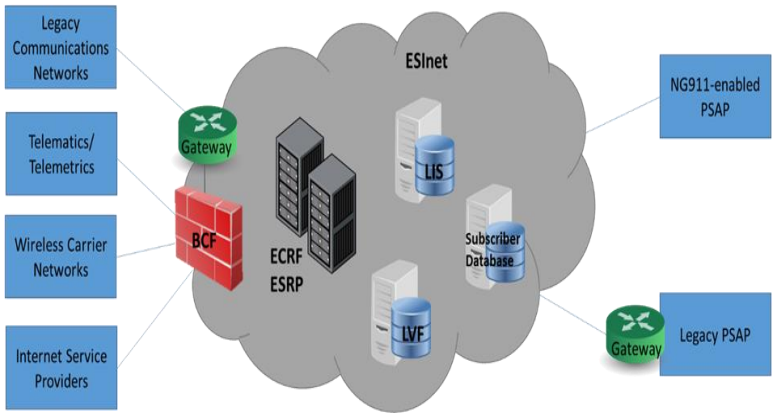

Figure B-1. Simplified ESInet Diagram

- **Applications and Databases.** NG9-1-1 uses a wide range of internal and external databases to support its services. Internal databases validate and route data, record call details, and enforce policy and business rules. External databases host many of the datasets that call takers and dispatchers rely on to provide improved accuracy and shortened response time, including GIS location data, government records, law enforcement records, healthcare information, and infrastructure data.

- **Standards and Security.** NG9-1-1 uses functions and protocols that are compliant with international IP standards, as well as standards developed within the emergency response community. NENA references Internet Engineering Task Force (IETF) IP standards when defining NG9-1-1.[7] In addition to NENA, there are several other entities that establish standards for NG9-1-1 systems, including the Association of Public-Safety Communications Officials (APCO), the Alliance for Telecommunications Industry Solutions (ATIS), and the IETF.[8] National Institute of Standards and Technology (NIST) Special Publication 800 and 1800 Series provide additional targeted cybersecurity guidance for PSAPs.

- **Human Processes.** In addition to next generation technologies, NG9-1-1 relies on human procedures and system operations procedures to manage and supervise its functionalities and effectiveness. Database establishment and maintenance procedures, IP network operations, security processes, troubleshooting procedures, database auditing, and accuracy validation procedures are just some examples of human processes involved with NG9-1-1.[9]

[7] The full list of NG9-1-1 functions, called the "i3" architecture, are defined in NENA 08-003, "Detailed Functional and Interface Standards for NG9-1-1." NENA has also defined security standard 75-001, "NENA Security for Next Generation 9-1-1 Standard (NG-SEC)." The i3 functions and standards, NG-SEC, and the full suite of other NG9-1-1 standards can be found at https://www.nena.org/?page=Standards.

[8] A full review of NG9-1-1 standards can be found on the National 911 Program's website at https://www.911.gov/pdf/National_911_Program_NG911_Standards_Identification_Analysis_2018.pdf.

[9] "What is NG9-1-1?" NENA. http://c.ymcdn.com/sites/www.nena.org/resource/resmgr/ng9-1-1_project/whatisng911.pdf.

Appendix C: Risk Terminology

Cybersecurity risks to Next Generation 9-1-1 (NG9-1-1) systems have severe potential consequences, including loss of life or property; job disruption for affected network users; and financial costs from the unauthorized use of data and subsequent resolution. To understand the significance of different risks to the confidentiality, integrity, or availability of NG9-1-1 systems, the terms *threat*, *vulnerability*, *likelihood*, and *consequence* must be understood.

Threats. Threats are anything that has the potential to harm the system and are produced by "threat actors." There are a variety of potential actors, each with different intent and capabilities to carry out an attack. By understanding the motivations and capabilities of those responsible for launching attacks, system administrators can better anticipate the types of attacks they might face and better protect data and assets that are likely targets. Threat actors who have caused real-world damage include, but are not limited to, those in Figure C-1:

- ✓ Anarchist……..Someone who rejects all forms of structure, private or public, and acts with few constraints
- ✓ Cyber Crime Ring……..Organized crime organization with significant cyber-attack resources
- ✓ Cyber Vandal…… Derives thrills from intrusion or destruction of property, without agenda
- ✓ Data Miner……...Professional data gatherer external to the company (includes cyber methods)
- ✓ Government Agent/Spy …. Foreign state-sponsored spy or agent as a trusted insider, supporting idealistic goals
- ✓ Government Cyberwarrior…Foreign state-sponsored attacker with significant resources to affect major disruption
- ✓ Nation-state…… A sovereign territory with significant resources to cause harm
- ✓ Radical Activist……Highly motivated, potentially destructive supporter of cause
- ✓ Terrorist…….. Person who relies on the use of violence to support personal socio-political agenda

Figure C-1. Threat Actors

In addition to attacks, unintentional threats can disrupt the confidentiality, integrity, or availability of NG9-1-1 systems. Unintentional threat actors include employees, vendors, contractors, or subcontractors. For example, one of these actors could:

- Improperly safeguard data when sending or storing (e.g., not using proper encryption, sending data to unauthorized individuals, putting weak protection on databases)
- Enter typing mistakes that result in loss of data integrity
- Accidentally make a data resource unavailable when performing maintenance or upgrade operations
- Not follow physical or cyber protection procedures
- Improperly test or maintain back-up systems and power sources

Vulnerabilities. Vulnerabilities are weaknesses in a system, network, or asset that could enable an undesired outcome, such as a network outage or security breach. Threat actors typically take advantage of databases or system applications with bad encryption, poor authorization and access control measures or policies, and interconnections or interfaces with an external network or entity. With numerous interconnections possible, PSAPs may suffer from vulnerabilities associated with systems for which they have not contributed funds, hold no direct authority, or provide other resources to support beyond network access and perhaps mutual-aid agreements—even if they share redundancies, databases, or other resources. Furthermore, different vendor implementations using proprietary technologies can lead to varying degrees of protection, even when addressing the same standards and system requirements.

Likelihood. Likelihood refers to the probability that a risk scenario could occur. Determining the likelihood of a risk depends on the level of both the threat and the vulnerability. It is the probability that a given threat type will exploit a set of vulnerabilities, resulting in the occurrence of a risk. For example, if a system has no vulnerabilities, the likelihood of risk is low even if there is a significant threat because the threat would have nothing to exploit. On the other hand, if the system contains a significant vulnerability but there is no threat to exploit it, the likelihood of a risk will be equally low. A risk with both a greater threat and greater vulnerability level is much more likely to occur than one with a low threat and low vulnerability level.

Consequences. While the potential consequences of cybersecurity breaches depend in large part on the type of breach, the severity of the breach is determined by its ability to impact and degrade NG9-1-1 systems and PSAP operations, or its ability to harm the citizens they serve and the public's confidence in 911 systems. Additional consequences include loss of sensitive records, including personal information about citizens, law enforcement data, critical infrastructure information, healthcare data, dispatch information, and legal liability for parties responsible for protecting the systems. When evaluating consequences, it is important for administrators to assume the worst possible outcome. For example, a data breach could be small, but administrators should account for the greatest reasonable consequence if that breach were to occur.

Because it is impossible to address every risk, it is helpful to look at which risks are more likely to occur to make more informed decisions about where to best allocate resources to ensure the most risk reduction. However, likelihood is only one part of the equation—the consequences of risks must also be assessed.

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

Appendix D: Public Safety and 9-1-1 Cyber Attack Examples

Threat Type	Description	Real World Example
Telephony-Denial-of-Service Attack (TDoS)	Use of Voice over Internet Protocol (VoIP) systems to overwhelm phone systems rendering them incapable of placing or receiving calls.	In October 2016, an Arizona teenager was charged with sending thousands of calls to 9-1-1 emergency call centers and law enforcement agencies in multiple states via compromised cell phones.[10]
Unauthorized Network Access	Attackers gain network access using stolen credentials and/or devices.	In 2016, two teenagers gained unauthorized access to the Manitowoc Police Department's Twitter account using stolen credentials.[11]
Unauthorized Data Access	Attackers can access sensitive databases (e.g., law enforcement, health records) to steal, modify, or corrupt the data.	In August 2017, Schuyler County in New York experienced a cyber-attack where hackers gained access to the communication system for the county through brute force cracking of passwords. The attack temporarily crippled the ability to dispatch deputies.[12]
Ransomware	Use of software to block computer systems for the purpose of extorting a ransom.	In March 2018, Baltimore City's 9-1-1 system was held hostage by ransomware. The attack compromised the city's computer-aided dispatch server, causing a temporary shutdown of the digital dispatch and recording systems.[13]
Swatting	Manipulation of IP-based 911 calls to indicate the call is originating from a location at which a most serious criminal act has taken or is taking place, prompting the local PSAP to dispatch a Special Weapons and Tactics (SWAT) team to the address.	In December 2017, a suspect from California wanted to swat his online video game opponent but got the wrong address. He called a Kansas jurisdiction to report a deadly hostage situation. When police arrived, a resident from that address tried to understand what happened but was shot during the confusion.[14]

[10] Tyler Paley, "MCSO: 18-Year-Old Arrested in Cyberattack on 911 System," *AZCentral*, October 27, 2016, https://www.azcentral.com/story/news/local/surprise-breaking/2016/10/27/phoenix-meetkumar-desai-arrested-cyberattack-911-system/92847226/.
[11] Patti Zarling, "Manitowoc Police: Texas Teens Behind Twitter Hack," *Herald Times Reporter*, January 20, 2017, https://www.htrnews.com/story/news/crime/2017/01/20/manitowoc-police-twitter-hack-texas-teens/96854032/.
[12] Joe Mahoney, "Upstate 911 System Crippled by Hacking," *Lockport Union-Sun & Journal*, September 7, 2017, http://www.lockportjournal.com/news/upstate-system-crippled-by-hacking/article_fe34ba8c-7113-5c94-a114-616bdc38386c.html.
[13] Kevin Rector, "Hack of Baltimore's 911 Dispatch System was Ransomware Attack, City Officials Say," *The Baltimore Sun*, March 28, 2018, http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-hack-folo-20180328-story.html.
[14] Nichole Manna, "Call of Duty Gaming Community Points to 'Swatting' in Deadly Wichita Police Shooting," *The Wichita Eagle*, December 29, 2017, http://www.kansas.com/news/local/crime/article192111974.html.

Appendix E: Acronym List

Acronym	Definition
CSIRT	Computer Security Incident Response Team
DDoS	Distributed-Denial-of-Service
ESInet	Emergency Services IP Network
IP	Internet Protocol
IRT	Incident Response Team
IT	Information Technology
LMR	Land Mobile Radio
NCCIC	National Cybersecurity and Communications Integration Center
NG9-1-1	Next Generation 9-1-1
PSAP	Public Safety Answering Point
SPOC	State Single Point of Contact
SWIC	Statewide Interoperability Coordinator
SWAT	Special Weapons and Tactics
TDoS	Telephony-Denial-of-Service
US-CERT	United States Computer Emergency Readiness Team
VoIP	Voice over Internet Protocol