Homeland Security

Office of Emergency Communications

Cyber Risks to Next Generation 911

The advent of Next Generation 911 (NG911) systems, which operate on an Internet Protocol (IP) platform, enables interconnection with a wide range of public and private networks, such as wireless networks, the Internet, and regular phone networks. NG911 systems will enhance the current capabilities of today's 911 networks, allowing compatibility with more types of communication, providing greater situational awareness to dispatchers and emergency responders, and establishing a level of resilience not previously possible. NG911 will allow Public Safety Answering Points (PSAPs) to accept and process a range of information from responders and the public alike, including real-time text, images, video, and voice calls. In addition, NG911 will provide PSAPs with supplemental location data, which may enable more effective response.

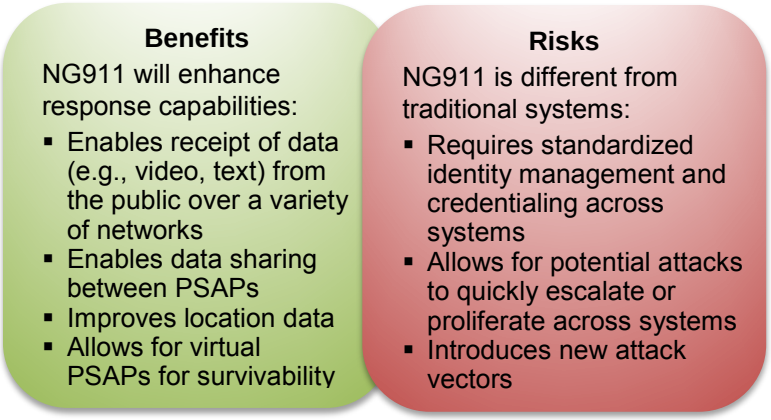

Figure 1: NG911 Benefits and Risks

Traditional 911 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 interconnections with other systems. The limited means of entry into the traditional 911 network significantly limited potential attack vectors, and what little cyber risk existed could be easily managed. NG911's interconnections enable new response capabilities, 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.

The potential cyber risks to a NG911 system do not undermine its tremendous benefits. Nevertheless, cyber risks do present a new level of exposure that PSAPs must understand and actively manage as a part of a comprehensive risk management program. Past events have proven 911 systems are attractive targets for cyber-attacks. For example, attackers have disrupted availability of traditional 911 systems by using auto-dialers to overwhelm PSAP phone lines and cause congestion, preventing legitimate 911 calls from going through [commonly called Telephone Denial of Service (TDoS) attacks] and location-based records and databases that support NG911 are of interest to cyber criminals, data miners, and even nation-states wanting to access and exploit that information.

As cyber threats grow in complexity and sophistication, attacks could be more severe against an NG911 system as attackers can launch multiple distributed attacks with greater automation from a broader geography against more targets. This issue paper provides an overview of NG911 cyber infrastructure, conveys the cyber risk landscape associated with NG911, offers an approach for assessing and managing risks, and provides additional NG911 resources.

Cyber Infrastructure

The National Emergency Number Association (NENA) describes NG911 systems as an IP-based system comprised of hardware, software, data, and operational policies and procedures that—

- Provides standardized interfaces from emergency call and message services;
- Processes all types of emergency calls, including voice, data, and multimedia information;
- Acquires and integrates additional emergency call data useful to call routing and handling;
- Delivers emergency calls, messages, and data to the appropriate PSAP and other entities;
- Supports data and communications needs for coordinated incident response and management; and
- Provides broadband service to PSAPs or other first responder entities.[1]

NENA defines several basic building blocks of NG911 systems, as described below:

- **Emergency Services IP Networks (ESInets).** ESInets are at the center of NG911 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.

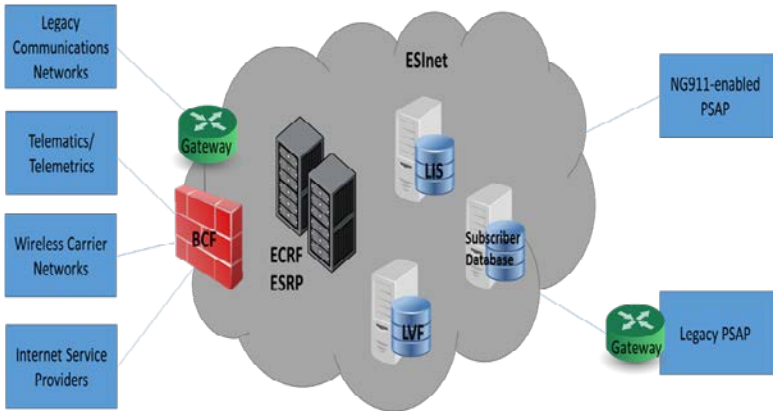

Figure 2: Simplified ESInet Diagram

- **Applications and Databases.** NG911 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 location data, government records, law enforcement records, healthcare information, and infrastructure data.
- **Standards and Security.** NG911 uses functions and protocols that are compliant with international IP standards, as well as standards developed within the emergency response community. NENA defines NG911 standards based on Internet Engineering Task Force (IETF) IP standards.[2] In addition to NENA, there are a number of other entities that establish standards for NG911 systems, including the Association of Public-Safety Communications Officials (APCO), the Alliance for Telecommunications Industry Solutions (ATIS), and the IETF.[3]

---

1 "What is NG911?". NENA. http://c.ymcdn.com/sites/www.nena.org/resource/resmgr/ng9-1-1_project/whatisng911.pdf.

2 The full list of NG911 functions, called the "i3" architecture, are defined in NENA 08-003, "Detailed Functional andInterface Standards for NG911." 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 NG911 standards can be found at https://www.nena.org/?page=Standards.

3 A full review of NG911 standards can be found on the National 911 Program's website at http://www.911.gov/pdf/NG911-Standards-Identification-and-Analysis-March2015.pdf.

> "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."
>
> National Infrastructure Protection Plan (2009, Revised and Updated 2013)

Per the definition above, cyber infrastructure for NG911 systems includes the IP-based networks, assets, databases, and services, as they are involved in the processing, storage, and transport of data. Specifically, an NG911 system's cyber infrastructure includes:

- Assets that are part of, or interconnect with, 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

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. NG911 administrators should recognize this convergence in order to more effectively counter risks. Risks to any component of these systems could threaten an entire NG911 system or its data, so it is important to consider systems holistically.

The NG911 Cybersecurity Risk Landscape

Cybersecurity[4] 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 three attributes most necessary for a secure system are often referred to as the C-I-A Triad:

- 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.
- Availability: Ensures that the infrastructure—either components of the network or the network as a whole—is operational and committable to its intended purpose.

The CIA Triad is used as a benchmark for evaluating information system security by the National Institute of Standards and Technology (NIST), the International Telecommunications Union (ITU), and others. Loss of confidentiality, integrity, or availability has especially severe impacts in the emergency response domain. For example, loss of confidentiality within NG911 systems could expose information to identity thefts or disrupt ongoing investigations; loss of integrity could disrupt response to 911 calls; and loss of availability could prevent urgent requests from reaching a PSAP.

[4] 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, 2009. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

Cybersecurity risks to NG911 systems, such as those shown in Figure 3, have severe potential impacts, including loss of life or property because of hampered response operations; job disruption for affected network users; substantial financial costs from the unauthorized use of data and subsequent resolution; and potential lawsuits from those whose data is breached or whose lives are adversely affected. To understand the significance of different risks to the confidentiality, integrity, or availability of a NG911 system, the terms threat,vulnerability, likelihood, and consequence must be understood.

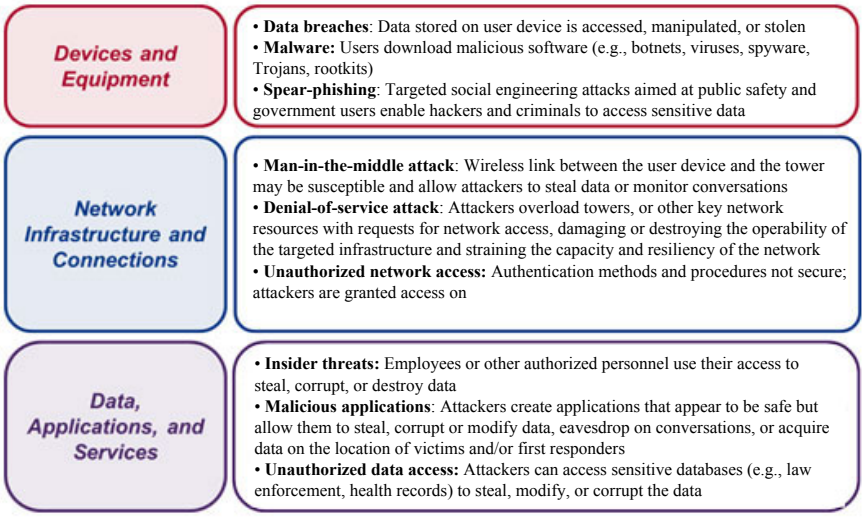

Figure 3: Potential Risks to NG911 System Components

Threats. Threats are anything that hasthe 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 4:

- ✓ Anarchist……..Someone who rejects all forms of structure, private or public, and acts with few constraints
- ✓ Cyber Criminal/Crime Ring……..Manager of organized crime organization with significant 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 4: Threat Actors

In addition to attacks, unintentional threats can disrupt the confidentiality, integrity, or availability of NG911 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. Vulnerabilities take two forms, those that are vulnerable to **external threats** and those that are vulnerable to **internal threats**. One of the key tactics of an attacker is to gain credentials and access to a network, and then exploit vulnerabilities within the network as a seemingly "trusted entity." Vulnerabilities can also be within a network and available to malicious threat actors who gain access to the internal system, either improperly (through hacking) or by misusing their current position (insider threats). These 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 vast interconnection possibilities, 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. In addition, different vendor implementations using proprietary technologies can lead to varying degrees of protection and interoperability, even when addressing the same standards and system requirements. Oversight of NG911 developments have focused primarily on deployment or modernization projects, but rarely on the governance and oversight of cyber risk management that are critical to cybersecurity.

Example Vulnerabilities

Old Systems: Systems that are out of date or past their lifecycle that lack modern security measures

Shared Systems: Shared systems/databases with other entities that have not employed security measures

Lack of Diversity and Redundancy: Lack of diverse routing for communications or redundancy for electric power decreases resilience

Lack of Security Policies: Ad hoc or non-existent security policies enable insiders to accidently or intentionally disrupt operations and/or security

Likelihood. Likelihood refers to the possibility that a risk scenario could occur. Determining the likelihood of a risk depends on the level of both the threat and the vulnerability and 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 NG911 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 possible legal liability for parties responsible for protecting the systems. When evaluating potential consequences, it is important for administrators to assume the worst possible outcome. For example, a particular type of data breach could be small and insignificant, but

administrators should account for the greatest reasonable consequence if that data 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

Improving NG911 Cybersecurity Posture

Given the dynamic nature of technology and the evolving cyber risk landscape, organizations should adopt a cybersecurity framework. An effective framework 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

Figure 4: NIST Framework Core Structure

The Department of Homeland Security (DHS) strongly recommends adopting the NIST Cybersecurity Framework, which is a flexible, risk-based approach to improving the security of critical infrastructure.[5] Collaboratively developed between government and the private sector, the framework is based on industry standards and best practices and can be used for NG911 systems. The NIST Cybersecurity Framework is designed to complement an existing cybersecurity risk management process or to develop a credible program if one does not exist. Figure 4 demonstrates the five core tenets of the NIST Framework: identify, protect, detect, respond, and recover. More information, including informative reference for addressing each tenet can be found in the Framework.

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

Identifying and Assessing Risks

Regardless of the cybersecurity framework chosen, administrators will need to identify, evaluate and prioritize risks for their organization. Figure 5 provides a sample risk assessment process.

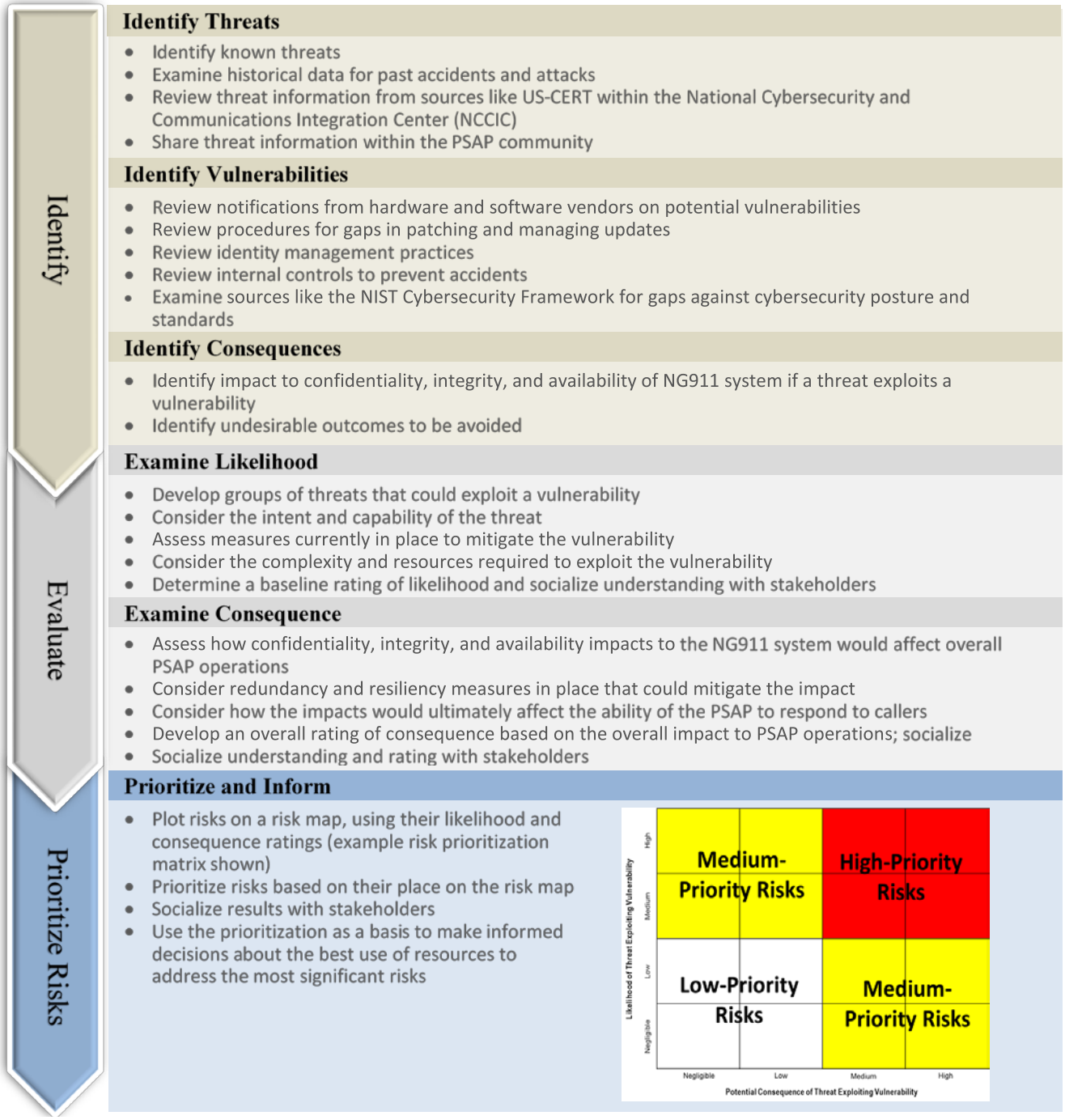

Figure 5: Sample Risk Assessment Plan (to be followed with mitigation and response/recovery)

Mitigating Risks: Protect and Detect

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

Table 1 describes sample mitigation strategies for NG911 cybersecurity. This list is not exhaustive and should not replace a comprehensive requirements analysis; however, it is intended to provide a starting point for requirements, planning, and implementation. Some elements may be addressed through nationwide standards, industry best practices, or policy guidance, while others may be developed and practiced by PSAP administrators.

Table 1: Sample NG911 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 to assist in carrying out cybersecurity planning. US-CERT is a CSIRT run by the DHS's National Cybersecurity and Communications Integration Center (NCCIC).[6] A CSIRT serves as a centralized location to report and analyze security issues within an organization. A CSIRT may also recommend potential solutions to the threats and publicize known threats, vulnerabilities, and solutions generally or to a specific information-sharing community. The CSIRT could also 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 the NG911 system and its data. In addition, 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. Sample response and recovery actions are shown in Figure 2.

Table 2: Sample NG911 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.** Establish an incident response team with 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[7].** 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

6 See: https://www.us-cert.gov/ccubedvp.

7 For continuity recommendations, see FEMA's Continuity Guidance Circular (CGC) 1 and 2 available at http://www.fema.gov/media-library/resources-documents/collections/343.

Actions for Improving NG911 Cybersecurity

This document provides an overview of the cyber risks that will be faced by NG911 systems. It is intended to serve only as an informational tool for system administrators to better understand the full scope and range of potential risks, as well as recommend mitigations to these risks. The following actions are provided for system administrators intending to improve their NG911 systems:

- **Adopt a "security first" perspective.** Cybersecurity has become an integral part of mission function and operations for NG911 systems. Working with others within the NG911 community, government, industry, and academia to establish consistent standards, policies, procedures, interoperability and implementation guidance for NG911 deployments is crucial.
- **Leverage historically-successful cybersecurity strategies.** Researching available references and resources, as well as gathering experiences from other NG911 community members, is important to constructing the ideal solution set for each NG911 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 within an organization. Tracking developments in the cybersecurity field and providing prioritized implementation of cybersecurity solutions are also CSIRT activities.
- **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.** This process should account for threats, vulnerabilities, and consequences associated with system assets. 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 in order to identify the full architecture of their system and assess it for physical and network vulnerabilities. This assessment should also include a review of their current processes and standard operating procedures against available government and industry cybersecurity best practices and standards.
- **Develop 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 available mitigation techniques and employing them in a prioritized fashion will produce a comprehensive cybersecurity solution.
- **Solidify Response and Recovery actions.** Establishing a CSIRT and developing incident response plans, policies, and capabilities for the networks, 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.

Once risks are identified and protection mitigations are in place, the NG911 community has an opportunity to focus on detection and advance planning. Instead of focusing on the individual cybersecurity events and data recovery, an effective framework uses data analytics in PSAPs, joint field offices, and emergency operations centers to accelerate and automate analysis, and to shift from a posture of "what just happened, and how do we fix it?" to "what is going to happen, and how can we prevent it?". The NG911 community should remain in front of potential cyber events through its ability to feed relevant event data to emergency operation centers, fusion centers, and cyber centers.

Resources

Table 3 provides a list of resources to assist NG911 administrators improving the cybersecurity posture of their systems.

Table 3: NG911 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 NG911 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. http://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. http://www.dhs.gov/national-cybersecurity-communications-integration-center
Federal Communications Commissions (FCC)	Legal and Regulatory Framework for NG911 Services	An overview on the development and creation of a NG911 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_WG4_Report_Final_March_18_2015.pdf
	Task Force on Optimal PSAP Architecture (TFOPA): Optimal Cybersecurity Approach for PSAPs	The TFOPA is a federal advisory committee chartered under the Federal Advisory Committee Act to provide recommendations to the FCC regarding actions that PSAPs can take to optimize their security, operations, and funding as they migrate to NG911. https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG1_FINAL_Report-121015.pdf
National 911 Program	911.gov	911.gov is a comprehensive resource for all things related to NG911. The website includes a resource center with an information clearinghouse, a Technical Assistance Center, and a 911 profile database for tracking the progress of 911 authorities around the Nation in enhancing their systems and deploying NG911 capabilities. www.911.gov
National Emergency Number Assoc. (NENA)	Standards (including i3 and NG-SEC)	NENA's website contains a complete archive of all its 911 standards, including those related to NG911, such as NG-SEC standard (NENA 75-001). https://www.nena.org/?page=Standards
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 NG911 system administrators manage cybersecurity-related risk. http://www.nist.gov/cyberframework/
	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. http://csrc.nist.gov/publications/PubsSPs.html#SP800