# 911 Cybersecurity Best Practices Package

Created for CC:IPS

Publication: July 2023
Cybersecurity and Infrastructure Security Agency

# Table of Contents

## PUBLIC SAFETY COMMUNICATIONS AND CYBER RESILIENCY TOOLKIT

The ability to maintain voice and data communications at all times is critical for public safety agencies to perform their life-saving missions. By establishing resiliency measures, public safety communications can better withstand potential disruptions to service.

The Cybersecurity and Infrastructure Security Agency (CISA) developed the Public Safety Communications and Cyber Resiliency Toolkit to assist public safety agencies and others responsible for communications networks in evaluating current resiliency capabilities, identifying ways to improve resiliency, and developing plans for mitigating the effects of potential resiliency threats.

To facilitate viewing available resources, an interactive graphic is provided.

- Topic specific systems-based resources appear as building shapes (blue); threats are cloud shapes (red).
- Clicking on a topic reveals a list of resources accompanied by a brief description.

The ability to maintain voice and data communications at all times is critical for public safety agencies to perform their life-saving missions. By establishing resiliency measures, public safety communications can better withstand potential disruptions to service.


## LINK TO THE INTERACTIVE TOOL: CISA PUBLIC SAFETY COMMUNICATIONS AND CYBER RESILIENCY TOOLKIT DRAFT (ADOBE.COM)

SAFECOM

NCSWIC

# THINGS EVERY 911 CENTER SHOULD DO TO IMPROVE CYBERSECURITY

911 CYBER ATTACK SURFACES

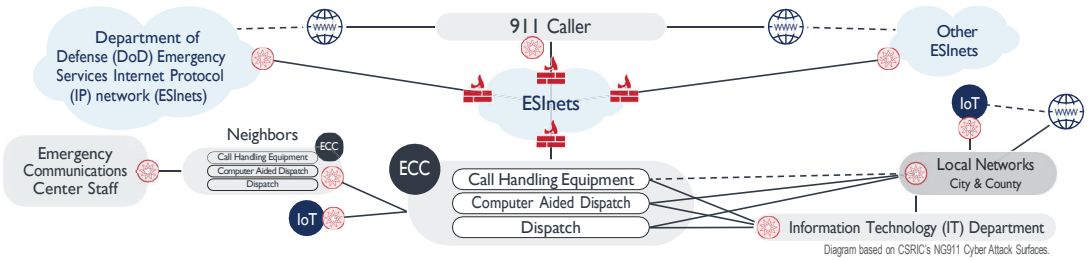



Diagram based on CSRIC's NG911 Cyber Attack Surfaces.

**The nation's most direct route to emergency assistance, the 911 system,** requires stable, safe, and resilient communications. Sophisticated criminal actors and nation-states exploit cyber vulnerabilities to threaten the delivery of essential services. The integration of new multimedia technology expands threat vectors. Increased interconnection of systems poses threats across a broader attack surface. Many of these new technologies are internet accessible, including critical mobile computing devices, such as DASEC, making them prevalent in open-source vulnerability scans.

Cybersecurity is a shared responsibility. All organizations play a role, and some organizations are being required to comply with standards, such as the National Fire Protection Association's (NFPA) Standard for Emergency Services Communications (NFPA 1225), to improve cybersecurity posture. SAFECOM, the National Council of Statewide Interoperability Coordinators (NCSWIC), the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), and other partners have resources to help. Cybersecurity has become an integral part of mission function and operations for legacy and Next Generation 911 (NG911) systems. Working with others within the community, government, industry, and academia to establish consistent standards, policies, procedures, interoperability, and implementation guidance for NG911 deployment is crucial.

## THINGS EVERY 911 CENTER CAN DO TO REDUCE CYBER RISKS

### CYBER RISK ASSESSMENT

Cybersecurity (cyber) risk assessments assist emergency communications centers (ECCs)/public safety answering points (PSAPs) in understanding vulnerabilities and threats to their operations (e.g., mission, functions, image, reputation), organizational assets, and individuals. A cyber risk assessment can help an ECC/PSAP determine next steps in protecting their systems and networks from malicious actors and infrastructure failures.

Below are resources that can help ECCs/PSAPs conduct cyber assessments

- SAFECOM, *Guide to Getting Started with a Cyber Risk Assessment*
- CISA, *Cyber Essentials Starter Kit: The Basics for Building a Culture of Cyber Readiness*
- CISA, *Public Safety Communications and Cyber Resiliency Toolkit*
- CISA, *Cyber Resiliency Resources for Public Safety Fact Sheet*
- NIST, *NIST Cybersecurity Framework*

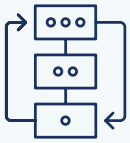
### CYBER INCIDENT RESPONSE AND VULNERABILITY RESPONSE PLANS

Cyber incident response and vulnerability response plans provide guidance on identifying, mitigating, responding to, and recovering from incidents that may impact ECC/PSAP systems and operations. It is key to ensure all users and devices, network infrastructure and connections, data, data applications,and services are fully assessed to prevent disruptions. An incident response plan is necessary to minimize gaps in services, prevent loss of data and services, and ensure continuity of operations.

Vulnerabilities should be identified with regular vulnerability scanning and Cyber Hygiene practices. Internet assessable vulnerabilities can be mitigated through implementation and maintenance of CISA's Cross-Sector Cybersecurity Performance Goals (CPGs). Cities can also enroll in CISA's no-cost Cyber Hygiene services to maintain awareness of vulnerabilities and take informed actions to reduce risk of compromise. Vulnerability response plans address steps to follow regarding identified cybersecurity threats and vulnerabilities. It is essential to coordinate with stakeholders and service providers to develop joint mutual agreements on continuity of operations during a crisis to include cyber attacks. Recovering data, testing, and training are critical components to response plans, and coordination with all stakeholders and partners can assist in a smooth transition.

Below are resources that can help ECCs/PSAPs develop cyber incident response plans:

- CISA, Federal Government Cybersecurity Incident and Vulnerability Response Playbooks
- CISA, *Essential Elements: Your Crisis Response* CISA, *Cyber Alerts*
- CISA, *Cyber Incident Response*



## HOW CAN OUR ECC/PSAP PARTICIPATE?

Perform regular cyber risk assessments and based on the findings:

- Develop incident and vulnerability response plans, recovery plans, and continuity of operations (COOP) plans to assist in cybersecurity incident response
- Exercise plans so they can be validated, refined, and updated
- Incorporate lessons learned into recovery planning processes and strategies
- Train response personnel on the latest security, resiliency, COOP, and operational practices and maintain in-service training as new technology and methods are made available
- Maintain coordination and communication with other partners, vendors, and stakeholders such as the Statewide Interoperability Coordinator (SWIC)
- Coordinate with service providers when developing and updating cyber response plans
- ECCs/PSAPs should consider implementing cyber threat detection and mitigation capabilities and using resources such as CISA capabilities and fusion centers. These state and local centers may provide system monitoring, threat identification, and intelligence sharing, allowing ECCs/PSAPs to maintain a proactive cyber posture
- Become familiar with Cyber Incident Response Case Studies and understand and prioritize threats that impact the agency's mission
- Consider implementing NG911 which maintains advanced authentication and enhanced security capabilities
- Enroll in CISA's no cost cyber hygiene services, such as vulnerability scanning, to maintain awareness of vulnerabilities and take informed actions to reduce risk of compromise
- Get your Stuff Off Search, reduce internet attack surfaces that are visible to anyone on web-based search platforms

# Cybersecurity Best Practices for Smart Cities

Publication: April 19, 2023

United States Cybersecurity and Infrastructure Security Agency
United States National Security Agency
United States Federal Bureau of Investigation
United Kingdom National Cyber Security Centre
Australian Cyber Security Centre
Canadian Centre for Cyber Security
New Zealand National Cyber Security Centre

## Summary

This guidance is the result of a collaborative effort from the United States Cybersecurity and Infrastructure Security Agency (CISA), the United States National Security Agency (NSA), the United States Federal Bureau of Investigation (FBI), the United Kingdom National Cyber Security Centre (NCSC-UK), the Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), and the New Zealand National Cyber Security Centre (NCSC-NZ). These cybersecurity authorities—herein referred to as "authoring organizations"—are aware that communities may seek cost-savings and quality-of-life improvements through the digital transformation of infrastructure to create "smart cities." In this context, the term "smart cities" refers to communities that:

- Integrate information and communications technologies (ICT), community-wide data, and intelligent solutions to digitally transform infrastructure and optimize governance in response to citizens' needs.
- Connect the operational technology (OT) managing physical infrastructure with networks and applications that collect and analyze data using ICT components—such as internet of things (IoT) devices, cloud computing, artificial intelligence (AI), and 5G.

Note: Terms that also refer to communities with this type of integration include "connected places," "connected communities," and "smart places." The communities adopting smart city technologies in their infrastructure vary in size and include university campuses, military installations, towns, and cities.

Integrating public services into a connected environment can increase the efficiency and resilience of the infrastructure that supports day-to-day life in our communities. However, communities considering becoming smart cities should thoroughly assess and mitigate the cybersecurity risk that comes with this integration. Smart cities are attractive targets for malicious cyber actors because of:

- The data being collected, transmitted, stored, and processed, which can include significant amounts of sensitive information from governments, businesses, and private citizens.
- The complex artificial intelligence-powered software systems, which may have vulnerabilities, that smart cities sometimes use to integrate this data.

The intrinsic value of the large data sets and potential vulnerabilities in digital systems means there is a risk of exploitation for espionage and for financial or political gain by malicious threat actors, including nation-states, cybercriminals, hacktivists, insider threats, and terrorists.

No technology solution is completely secure. As communities implement smart city technologies, this guidance provides recommendations to balance efficiency and innovation with cybersecurity, privacy protections, and national security. Organizations should implement these best practices in alignment with their specific cybersecurity requirements to ensure the safe and secure operation of infrastructure systems, protection of citizens' private data, and security of sensitive government and business data.

The authoring organizations recommend reviewing this guidance in conjunction with NCSC-UK's Connected Places Cyber Security Principles, ACSC's An Introduction to Securing Smart Places, CCCS's Security Considerations for Critical Infrastructure, CISA's Cross-Sector Cybersecurity Performance Goals, Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default, and Protecting Against Cyber Threats to Managed Service Providers and their Customers.

## Risk to Smart Cities

Smart cities may create safer, more efficient, more resilient communities through technological innovation and data-driven decision-making; however, this opportunity also introduces potential vulnerabilities that, if exploited, could impact national security, economic security, public health and safety, and critical infrastructure operations. Cyber threat activity against OT systems is increasing globally, and the interconnection between OT systems and smart city infrastructure increases the attack surface and heightens the potential consequences of compromise.

Smart cities are an attractive target for criminals and cyber threat actors to exploit vulnerable systems to steal critical infrastructure data and proprietary information, conduct ransomware operations, or launch destructive cyberattacks. Successful cyberattacks against smart cities could lead to disruption of infrastructure services, significant financial losses, exposure of citizens' private data, erosion of citizens' trust in the smart systems themselves, and physical impacts to infrastructure that could cause physical harm or loss of life. Communities implementing smart city technologies should account for these associated risks as part of their overall risk management approach. The authoring organizations recommend the following resources for guidance on cyber risk management:

- An introduction to the cyber threat environment (CCCS)
- Control System Defense: Know the Opponent (CISA, NSA)
- Cyber threat bulletin: Cyber threat to operational technology (CCCS)
- Cyber Assessment Framework (NCSC-UK)

### Expanded and Interconnected Attack Surface

Integrating a greater number of previously separate infrastructure systems into a single network environment expands the digital attack surface for each interconnected organization. This expanded attack surface increases the opportunity for threat actors to exploit a vulnerability for initial access, move laterally across networks, and cause cascading, cross-sector disruptions of infrastructure operations, or otherwise threaten confidentiality, integrity, and availability of organizational data, systems, and networks. For example, malicious actors accessing a local government IoT sensor network might be able to obtain lateral access into emergency alert systems if the systems are interconnected.

Additionally, as a result of smart cities integrating more systems and increasing connectivity between subnetworks, network administrators and security personnel may lose visibility into collective system risks. This potential loss of visibility includes components owned and operated by vendors providing their infrastructure as a service to support integration. It is critical that system owners maintain awareness and control of the evolving network topology as well as the individuals/vendors responsible for the overall system and each segment. Ambiguity regarding roles and responsibilities could degrade the system's cybersecurity posture and incident response capabilities. Communities implementing smart city technology

should assess and manage these risks associated with complex interconnected systems.

## Risks From the ICT Supply Chain and Vendors

Communities building smart infrastructure systems often rely on vendors to procure and integrate hardware and software that link infrastructure operations via data connections. Vulnerabilities in ICT supply chains—either intentionally developed by cyber threat actors for malicious purposes or unintentionally created via poor security practices—can enable:

- Theft of data and intellectual property,
- Loss of confidence in the integrity of a smart city system, or
- A system or network failure through a disruption of availability in operational technology.

ICT vendors providing smart city technology should take a holistic approach to security by adhering to secure-by-design and secure-by-default development practices. Software products developed in accordance with these practices decrease the burden on resource-constrained local jurisdictions and increase the cybersecurity baseline across smart city networks. See the following resource for guidance on secure-by-design and secure-by-default development practices:

- Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default (CISA, NSA, FBI, ACSC, NCSC-UK, CCCS, BSI, NCSC-NL, CERT NZ, NCSC-NZ)

The risk from a single smart city vendor could be much higher than in other ICT supply chains or infrastructure operations, given the increased interdependencies between technologies and basic or vital services. Organizations should consider risks from each vendor carefully to avoid exposing citizens, businesses, and communities to both potentially unreliable hardware and software and deliberate exploitation of supply chain vulnerabilities as an attack vector. This includes scrutinizing vendors from nation-states associated with cyberattacks, or those subject to national legislation requiring them to hand over data to foreign intelligence services.

Illicit access gained through a vulnerable ICT supply chain could allow the degradation or disruption of infrastructure operations and the compromise or theft of sensitive data from utility operations, emergency service communications, or visual surveillance technologies. Smart city IT vendors may also have access to vast amounts of sensitive data from multiple communities to support the integration of infrastructure services—including sensitive government information and personally identifiable information (PII)—which would be an attractive target for malicious actors. The aggregation of sensitive data may provide malicious actors with information that could expose vulnerabilities in critical infrastructure and put citizens at risk. See the following resources for guidance on mitigating supply chain risks:

- Information and Communications Technology Supply Chain Risk Management (CISA)
- Supply chain security guidance (NCSC-UK)

- Identifying Cyber Supply Chain Risks (ACSC)
- Cyber supply chain: An approach to assessing risk (CCCS)

### Automation of Infrastructure Operations

Smart cities can achieve efficiencies by automating operations, such as wastewater treatment or traffic management. Automation reduces the requirement for direct human control of those systems. Automation can also allow for better consistency, reliability, and speed for standardized operations. However, automation can also introduce new vulnerabilities because it increases the number of remote entry points into the network (e.g., IoT sensors and remote access points). The volume of data and complexity of automated operations—including reliance on third-party vendors to monitor and manage operations—can reduce visibility into system operations and potentially hinder real-time incident response.

Automation for infrastructure operations in smart city environments may require the use of sensors and actuators that increase the number of endpoints and network connections that are vulnerable to compromise. The integration of AI and complex digital systems could introduce new unmitigated attack vectors and additional vulnerable network components. Reliance on an AI system or other complex systems may decrease overall transparency into the operations of networked devices as these systems make and execute operational decisions based on algorithms instead of human judgment.

## Recommendations

### Secure Planning and Design

The authoring organizations strongly recommend communities include strategic foresight and proactive cybersecurity risk management processes in their plans and designs for integrating smart city technologies into their infrastructure systems. New technology should be deliberately and carefully integrated into legacy infrastructure designs. Communities should ensure any "smart" or connected features they are planning to include in new infrastructure are secure by design and incorporate secure connectivity with any remaining legacy systems. Additionally, communities should be aware that legacy infrastructure may require a redesign to securely deploy smart city systems. Security planning should focus on creating resilience through defense in depth and account for both physical and cyber risk as well as the converged cyber-physical environment that IoT and industrial IoT (IIoT) systems introduce. See the following consolidated, baseline practices that organizations of all sizes can implement to reduce the likelihood and impact of known IT and OT risks.

- Cross-Sector Cybersecurity Performance Goals (CISA)

See the following additional resources for guidance on accounting for risks in the cyber, physical, and converged environments:

- Improving ICS Cybersecurity with Defense-in-Depth Strategies (CISA)

- Cybersecurity and Physical Security Convergence (CISA)
- Consequence-Driven Cyber-Informed Engineering (INL)

### *Apply the principle of least privilege.*

The organizations responsible for implementing smart city technology should apply the principle of least privilege throughout their network environments. As defined by the U.S. National Institute of Standards and Technology (NIST), the principle of least privilege is, "The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function." Administrators should review default and existing configurations along with hardening guidance from vendors to ensure that hardware and software is only permissioned to access other systems and data that it needs to perform its functions. Administrators should also immediately update privileges upon changes in administrative roles or the addition of new users or administrators from newly integrated systems. They should use a tiered model with different levels of administrative access based on job requirements. Administrators should limit access to accounts with full privileges across an enterprise to dedicated, hardened privileged access workstations (PAWs). Administrators should also use time-based or just-in-time privileges and identify high-risk devices, services, and users to minimize their access. For detailed guidance, see:

- Defend Privileges and Accounts (NSA)
- Restricting Administrative Privileges (ACSC)
- Managing and controlling administrative privileges (CCCS)

### *Enforce multifactor authentication.*

The organizations responsible for implementing smart city technology should secure remote access applications and enforce multifactor authentication (MFA) on local and remote accounts and devices where possible to harden the infrastructure that enables access to networks and systems. Organizations should explicitly require MFA where users perform privileged actions or access important (sensitive or high-availability) data repositories. Russian state-sponsored APT actors have recently demonstrated the ability to exploit default MFA protocols. Organizations responsible for implementing smart cities should review configuration policies to protect against "fail open" and re-enrollment scenarios. See the following resource for guidance on implementing MFA:

- #More Than a Password (CISA)
- Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability (FBI, CISA)
- Transition to Multi-Factor Authentication (NSA)
- MFA for online services (NCSC-UK)
- Implementing MFA (ACSC)

- Zero trust architecture design principles - Authenticate and authorize (NCSC-UK)

### *Implement zero trust architecture.*

Implementing zero trust network design principles will create a more secure network environment that requires authentication and authorization for each new connection with a layered, defense-in-depth approach to security. Zero trust also allows for greater visibility into network activity, trend identification through analytics, issue resolution through automation and orchestration, and more efficient network security governance. See the following resources for guidance on implementing zero trust:

- Zero trust architecture design principles (NCSC-UK)
- Zero Trust Maturity Model (CISA)
- Embracing a Zero Trust Security Model (NSA)
- A zero trust approach to security architecture (CCCS)
- Zero Trust security model (CCCS)

Note: Both zero trust architecture and MFA should be applied wherever operationally feasible in balance with requirements for endpoint trust relationships. Some OT networks may require trust-by-default architectures, but organizations should isolate such networks and ensure all interconnections with that network are secured using zero trust and related principles.

### *Manage changes to internal architecture risks.*

The organizations responsible for implementing smart city technology should understand their environment and carefully manage communications between subnetworks, including newly interconnected subnetworks linking infrastructure systems. Network administrators should maintain awareness of their evolving network architecture and the personnel accountable for the security of the integrated whole and each individual segment. Administrators should identify, group, and isolate critical business systems and apply the appropriate network security controls and monitoring systems to reduce the impact of a compromise across the community. See the following resources for detailed guidance:

- CISA Vulnerability Scanning (CISA)
- Vulnerability Scanning Tools and Services (NCSC-UK)
- Security architecture anti-patterns (NCSC-UK)
- Preventing Lateral Movement (NCSC-UK)
- Segment Networks and Deploy Application-aware Defenses (NSA)

### *Securely manage smart city assets.*

Secure smart city assets against theft and unauthorized physical changes. Consider implementing physical and logical security controls to protect sensors and monitors against manipulation, theft, vandalism, and environmental threats.

### *Improve security of vulnerable devices.*

See the following resources for guidance on protecting devices by securing remote access:

- Selecting and Hardening Remote Access VPN Solutions (CISA, NSA)
- Using Virtual Private Networks (ACSC)
- Virtual private networks (CCCS)

### *Protect internet-facing services.*

See the following resources for guidance on protecting internet-facing services:

- Protecting internet-facing services on public service CNI (NCSC-UK)
- Strategies for protecting web application systems against credential stuffing attacks (CCCS)
- Isolate web-facing applications (CCCS)

### *Patch systems and applications in a timely manner.*

Where possible, enable automatic patching processes for all software and hardware devices that include authenticity and integrity validation. Leverage threat intelligence to identify active threats and ensure exposed systems and infrastructure are protected. Secure software assets through an asset management program that includes a product lifecycle process. This process should include planning replacements for components and software nearing or past end-of-life, as patches may cease to be developed by manufacturers or developers. See the following resources for guidance on protecting systems and networks via asset management:

- Known Exploited Vulnerabilities Catalog (CISA)
- Asset management for cyber security (NCSC-UK)

### *Review the legal, security, and privacy risks associated with deployments.*

Implement processes that continuously evaluate and manage the legal and privacy risks associated with deployed solutions.

## Proactive Supply Chain Risk Management

All organizations responsible for implementing smart city technology should proactively manage ICT supply chain risk for any new technology, including hardware or software that supports the implementation of smart city systems or service providers supporting implementation and operations. Organizations should use only trusted ICT vendors and components. The ICT supply chain risk management process should include participation from all levels of the organization and have full support from program leaders implementing smart city systems. Procurement officials from communities implementing smart city systems should also communicate minimum security requirements to vendors and articulate actions they will take in response to breaches of those requirements. Smart city technology supply chains should be transparent to the citizens whose data the systems will collect and process.

For detailed supply chain security guidance, see:

- Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (CISA, ACSC, NCSC-NZ, NCSC-UK, CCCS)
- Supply chain security guidance (NCSC-UK)
- ICT Supply Chain Library (CISA)
- Cyber-Physical Security Considerations for the Electricity Sub-Sector (CISA)
- Cyber Supply Chain Risk Management (ACSC)

### *Software Supply Chain*

The organizations responsible for implementing smart city technology should set security requirements or controls for software suppliers and ensure that potential vendors use a software development lifecycle that incorporates secure development practices, maintains an active vulnerability identification and disclosure process, and enables patch management.

Product vendors should also assume some of the risk associated with their products and develop smart city technology in adherence to secure-by-design and secure-by-default principles and active maintenance for the products they provide. Vendors adhering to these principles give the organizations responsible for procuring and implementing smart city technology more confidence in the products they introduce into their networks.

For detailed guidance, see:

- Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default (CISA, NSA, FBI, ACSC, NCSC-UK, CCCS, BSI, NCSC-NL, CERT NZ, NCSC-NZ)
- Software Bill of Materials (CISA)
- Supply Chain Cyber Security: In Safe Hands (NCSC-NZ)
- Securing the Software Supply Chain: Recommended Practices Guide for Customers (ODNI, NSA, CISA, CSCC, DIBSCC, ITSCC)
- Coordinated Vulnerability Disclosure Process (CISA)
- Protecting your organization from software supply chain threats (CCCS)

### *Hardware and IoT Device Supply Chain*

Organizations responsible for implementing smart city technology should determine whether the IoT devices and hardware that will enable “smart” functionality will require support from third-party or external services. These organizations should perform due-diligence research on how parts are sourced and assembled to create products. They should also determine how the devices store and share data and how the devices secure data at rest, in transit, and in use. Organizations should maintain a risk register that identifies both their own and their vendors’ reliance on cloud computing support, externally sourced components, and similar dependencies. For detailed guidance, see:

- Cyber supply chain: An approach to assessing risk (CCCS)
- Cybersecurity for IOT Program (NIST)
- Defending Against Software Supply Chain Attacks (CISA, NIST)

### *Managed Service Providers and Cloud Service Providers*

Organizations should set clear security requirements for managed service providers and other vendors supporting smart city technology implementation and operations. Organizations should account for the risks of contracting with third-party vendors in their overall risk management planning and ensure organizational security standards are included in contractual agreements with external parties. Similarly, organizations should carefully review cloud service agreements, including data security provisions and responsibility sharing models. For detailed guidance, see:

- Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default (CISA, NSA, FBI, ACSC, NCSC-UK, CCCS, BSI, NCSC-NL, CERT NZ, NCSC-NZ)
- Protecting Against Cyber Threats to Managed Service Providers and their Customers (NCSC-UK, CCCS, NCSC-NZ, CISA, NSA, FBI)
- Six steps toward more secure cloud computing (FTC)
- Choosing the best cyber security solution for your organization (CCCS)

## Operational Resilience

The organizations responsible for implementing smart city technology should develop, assess, and maintain contingencies for manual operations of all critical infrastructure functions and train staff accordingly. Those contingencies should include plans for disconnecting infrastructure systems from one another or from the public internet to operate autonomously. In the event of a compromise, organizations should be prepared to isolate affected systems and operate other infrastructure with as little disruption as possible.

### *Backup systems and data.*

The organizations responsible for implementing smart city technology should create, maintain, and test backups, both for IT system records and for manual operational capabilities for the physical systems integrated in a smart city network. These organizations should identify how and where data will be collected, processed, stored, and transmitted and ensure each node in that data lifecycle is protected. System administrators should store IT backups separately and isolate them to inhibit the spread of ransomware—many ransomware variants attempt to find and encrypt/delete accessible backups. Isolating backups enables restoration of systems/data to their previous state in the case of a ransomware attack.

The organizations responsible for implementing smart city technology should have plans in place and training for staff so operations managers can disconnect normally connected infrastructure systems and operate manually in an "offline" mode to maintain basic service levels. For detailed guidance, see:

- Offline backups in an online world (NCSC-UK)

### *Conduct workforce training.*

Though implementation of smart city technology may include extensive automation, employees responsible for managing infrastructure operations should be prepared to isolate compromised IT systems from OT and manually operate core functions if necessary. Organizations should train new and existing employees on integrated, automated operations as well as isolated, manual backup procedures, including processes for restoring service after a restart. Organizations should update training regularly to account for new technologies and components. For detailed guidance, see:

- ICS Training Available Through CISA (CISA)

### *Develop and exercise incident response and recovery plans.*

Incident response and recovery plans should include roles and responsibilities for all stakeholders including executive leaders, technical leads, and procurement officers from inside and outside the smart city implementation team. The organizations responsible for implementing smart city technology should maintain up-to-date and accessible hard copies of these plans for responders should the network be inaccessible (e.g., due to a ransomware attack). Organizations should exercise their plans annually and coordinate with continuity managers to ensure continuity of operations. For detailed guidance see:

- Incident Response Plan Basics (CISA)
- Effective steps to cyber exercise creation (NCSC-UK)
- Incident Management: Be Resilient, Be Prepared (NCSC-NZ)
- Preparing for and Responding to Cyber Security Incidents (ACSC)
- Developing your incident response plan (CCCS)
- Developing your IT recovery plan (CCCS)

## Purpose

This guidance was developed by U.S., U.K., Australian, Canadian, and New Zealand cybersecurity authorities to further their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations.

## Acknowledgements

Microsoft, IBM, and Nozomi Networks contributed to this guidance.

## Disclaimer

The information in this report is provided "as is" for informational purposes only. CISA, NSA, FBI, NCSC-UK, ACSC, CCCS, and NCSC-NZ do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise does not constitute or imply endorsement, recommendation, or favoring.

## Contact Information

U.S. organizations: report incidents and anomalous activity to CISA 24/7 Operations Center at report@cisa.gov or (888) 282-0870 and/or to the FBI via your local FBI field office, the FBI's 24/7 CyWatch at (855) 292-3937, or CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. United Kingdom organizations: report a significant cyber security incident at ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973. Australian organizations: visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and to access alerts and advisories. Canadian organizations: report incidents by emailing CCCS at contact@cyber.gc.ca. New Zealand organizations: report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.

# PROTECT YOUR CENTER FROM RANSOMWARE

PLACE STATE AGENCY/DEP/DIV LOGO OR SEAL

## [INSERT NAME OF STATE AGENCY /DEPT/DIVISION]

### RANSOMWARE: WHAT IS IT?

Ransomware is a type of malicious software (a.k.a malware) that cyber criminals use to extort money from organizations. When activated, ransomware encrypts information stored on your computer and attached network drives, and demands a ransom payment in exchange for the decryption key.

Ransomware attacks are costly and disruptive; there are serious risks to consider before paying ransom. The Federal Government does not recommend paying ransom. When organizations are faced with an inability to function, they must evaluate all options to protect themselves and their operations.

### IF YOU BELIEVE YOUR COMPUTER IS INFECTED WITH MALWARE

1. **Contact your IT department and supervisor immediately**
2. **If you can locate the Ethernet cable, unplug the computer from the network**
3. **If you can't disconnect the computer from the network, unplug it from power**

   *For laptops: hold down the power button until the light is completely off and remove the battery if possible*

### WHY ARE PSAPS A TARGET?

Emergency communications operations are crucial to public health and safety; interruptions in service could result in loss of life. Because they are so important, public safety answering points (PSAPs) and emergency communications centers (ECCs) are high-value targets for cyber threat actors.

**Note To Users:**

***Talk with your IT manager for guidance on running software and operating system updates. These updates include the latest security patches, making it harder for cybercriminals to compromise your computer.***

***The Federal Government advises organizations NOT to pay any ransom. Organizations should maintain off-site, tested backups of critical data.***

## IMPORTANT CONTACTS

*If your center has experienced a ransomware attack or any other malicious cybersecurity activity, the following contacts may provide assistance*

### STATE OF [INSERT NAME]

- [Insert Contact Name] [Insert Contact #]
- [Insert Contact Name] [Insert Contact #]
- [Insert Contact Name] [Insert Contact #]

### FEDERAL PARTNERS

- Cybersecurity and Infrastructure Security Agency (CISA) (888) 282-0870 www.cisa.gov
- Multi-State Information Sharing and Analysis Center® (MS-ISAC®) (866) 787-4722
- FBI [Insert City Name] Field Office [Insert local FBI FO contact #]
- FBI Internet Crime Complaint Center (IC3) www.ic3.gov
- FBI Field Office Cyber Task Forces http://www.fbi.gov/contact-us/field

To receive an agency-specific customized PSAP Ransomware Poster, Statewide Interoperability Coordinators (SWIC) can contact their CISA Emergency Communications Coordinator or email ecd@cisa.dhs.gov.

## PROTECTING YOUR CENTER

***Practice cyber awareness and complete all required cybersecurity training. Knowing and following your organization's cybersecurity policies is key to protecting your center.***

### PHISHING

***Attackers will send emails enticing users to open an attachment or click a link. Taking either action will lead to ransomware infection.***

- ☑ Be suspicious of any email asking you to follow a link or open an attachment
- ☑ If you are not expecting an email attachment from a co-worker, give them a call to verify
- ☑ Report suspicious emails to your IT staff
- ☑ Never check personal email from computer with access to CAD, RMS, or other mission critical system
- ☑ Hover over a hyperlink with your mouse to see the hyperlink address. If the written hyperlink and the one shown when hovering are different— this is a red flag
- ☑ Avoid clicking in pop-ups. Attackers use pop-ups to entice users to click on pop-up windows which may trigger malicious software

### SOCIAL ENGINEERING

***Attackers use social engineering to trick you into disclosing confidential information or clicking a malicious link. They study your "digital footprint" (e.g. social media accounts) and create emails designed to exploit your trusted relationships.***

- ☑ Remove any work-related information from your social media accounts
- ☑ Be suspicious of emails or phone calls from management asking you to do something outside of protocol or procedure
- ☑ Be suspicious of emails from coworkers and friends asking you to click a link or open an attachment

### DRIVE-BY-DOWNLOAD

***Attackers will host ransomware on websites or through advertising networks. Just visiting a malicious site will enable malware or ransomware infection.***

- ☑ Never browse the internet from a computer with access to CAD, RMS, or other mission critical system
- ☑ If your center has a designated computer for internet browsing, check with IT to ensure that your computer and web browser are up-to-date, and pop-up blocking is enabled
- ☑ Web browsing should be limited to websites related to your mission and job responsibilities

### USERNAME & PASSWORD COMPROMISE

***Attackers can use compromised usernames and passwords to log on to your workstation remotely, or gain acces to your agency's network. If your password is too simple, it can also be easily guessed.***

- ☑ Use complex passwords that include upper and lower case letters, special characters, and numbers, or use a 3-4 word pass-phrase if the option is available
- ☑ Don't reuse passwords across different accounts and online services
- ☑ Don't share passwords with other users, post passwords within the center, or save work-related passwords on your personal devices

### INFECTED USB DEVICES (USB Sticks, Thumbdrives, Smartphones, Etc)

***Ransomware can infect a computer when a user attaches an infected USB device. Attackers may leave thumbdrives in public places hoping you will insert them into your computer.***

- ☑ Never connect USB devices to CAD, RMS, or other mission critical systems
- ☑ Never charge any smartphone via a USB connection on CAD, RMS, or other mission critical systems; use a wall outlet

# Cyber Incident Response to Public Safety Answering Points: A State's Perspective

## Background

Public safety answering points (PSAPs) are increasingly being targeted by malicious actors seeking to disrupt emergency communications systems and operations. Across the country, PSAPs with varying levels of resources and response capabilities are facing complex and sophisticated cyberattacks.[1]

This case study highlights one state's response to cyber incidents involving PSAPs, including the legislation surrounding their authority, the collaboration required for a successful response, and best practices for entities preparing for cyberattacks. The Cybersecurity and Infrastructure Security Agency (CISA), SAFECOM, and National Council of Statewide Interoperability Coordinators (NCSWIC) collaborated with state public safety and emergency communications stakeholders to develop the case study and share lessons learned from responding to cyber incidents. This document provides actionable tips to help emergency communications centers (ECCs)/PSAPs prepare for and respond to cyber incidents.

## Governance

To better respond to cyber incidents, the state governor signed an executive order establishing a cybersecurity integration center (CIC). Two years after the executive order was signed it became law, providing funding to expand the center's cybersecurity capabilities, including additional staff for intelligence, operations, and incident support.

The CIC is comprised of state agencies, including police, information technology (IT), emergency services, the military department, and local and federal partners, such as CISA and the Federal Bureau of Investigation (FBI). These agencies have established relationships and pre-determined responsibilities to engage in CIC-assisted cyber incident response and recovery.

## Response

To address cyber threats, the state's governance document outlines processes for reporting and responding to cyber incidents. The state has IT personnel available 24 hours a day for PSAPs to report incidents and outages. When a PSAP reports an incident, it is processed using an incident report, given an escalation rating using a scale of one to five, classified by the type of incident, and then assigned to the appropriate agency or department for further assistance.

Information about the reporting PSAP, type of threat, and systems impacted are used to determine the state's response. An example timeline of a larger cyber incident response is as follows:

---

[1] CISA's *Transition to Next Generation 911 (NG911)* web page provides resources and best practices for ECCs/PSAPs to secure NG911 systems.


After an entity reports a cyber incident, the first phase of response is to gather information on the specifics of the attack and system attributes.


The second phase is to develop an incident-specific response plan and identify any resources needed. The response varies depending on the needs and capabilities of the reporting entity, as some larger agencies have additional resources available.


By phase three, the state response team is deployed for on-site assistance and forensic evidence collection. As a condition of the state's response, they require a representative from the PSAP to be on-site 24 hours a day to assist as needed.

State-level response can vary depending on the criticality and complexity of the incident. For more complex incidents, the on-site response is typically one to two weeks to identify and respond to the cyber threat. They may provide the PSAP with:

- On-site support
- Recommended points of contact to assist with remediation efforts
- Assistance brokering between the PSAP and their cybersecurity insurance provider, if applicable

For long-term events, the state response team supplements their staffing plan to prevent burn out. This is especially important if there are simultaneous attacks. In these cases, the state engages with partners, such as the National Guard, to assist with response operations and implements a staffing rotation plan. The state works collaboratively with partners to identify potential threats, share intelligence, and provide no-cost scans of an agency's networks.

## Future Plans

The state is currently developing a case management system to capture metrics on cyberattacks to help identify trends and threats. They are also developing a cloud-based incident reporting system for entities to report incidents and submit tickets through a mobile application or by phone. Additionally, they plan to increase capacity to deploy rapid incident response teams to incident sites.

## Lessons Learned

### Develop strong cyber incident response and vulnerability response plans

ECCs/PSAPs should develop cyber incident response and vulnerability response plans. Cyber incident response and vulnerability response plans can provide agencies with a roadmap to follow during cyber incidents to minimize confusion. These plans should include up-to-date contact lists and detailed steps for agencies to take in the event of an incident. Staff should be trained on cyber incident response. Plans should be tested (e.g., tabletop exercises) and updated regularly.

## Provide incident reporting 24 hours a day, 7 days a week, 365 days a year

Cyber incidents are not limited to normal working hours. ECCs/PSAPs should consider the need for on-call support, especially for incidents that take place after business hours, on weekends, or holidays. The ability to contact live, real-time support to walk through next steps can mitigate damage and improve response and recovery.

## Establish relationships with partners prior to a cyber incident

Responding to cyber incidents involves collaboration across multiple agencies. ECCs/PSAPs should establish relationships with partners prior to an attack to help ensure a seamless response. These relationships may include service providers, neighboring agencies, and state, local, and federal agencies. Including partners in exercises, trainings, and response plan development helps ensure agencies and partners are familiar with their roles and responsibilities responding to a cyber incident.

## Document network systems and architecture

ECCs/PSAPs should maintain awareness of their networks and assets, including hardware and software inventories and information regarding internal and external network connectivity. Familiarity with architecture and systems can greatly improve response effectiveness and timeliness because it reduces the time needed for responding agencies to gain knowledge about the network prior to gathering evidence and identifying and responding to a threat. It is recommended that ECCs/PSAPs know who has access to systems, ensure there is a business need, and establish user access agreements to outline user permissions and expectations. ECCs/PSAPs should proactively review vendor contracts, agreements, and data to define how data is handled, vendor infrastructure and practices the vendor utilizes, and each vendor's responsibilities in an incident.

## Practice good cyber hygiene to reduce the risk of cyberattacks

ECCs/PSAPs should implement good cyber hygiene in their daily operations, through the use of CISA provided resources, such as the *Public Safety Communications and Cyber Resiliency Toolkit*, and enrollment in no-cost Cyber Hygiene Services. ECCs/PSAPs should consider developing or refining authentication and password policies including strong, unique passwords requirements and multi-factor authentication, where possible. ECC's and PSAPS can also enroll in CISA's no-cost Cyber Hygiene services, such as Vulnerability Scanning, to maintain awareness of vulnerabilities and take informed actions to reduce risk of compromise.

## Implement cyber threat detection capabilities

ECCs/PSAPs should consider implementing cyber threat detection and mitigation capabilities and using resources such as fusion centers. These state and local centers may provide system monitoring, threat identification, and intelligence sharing, allowing ECCs/PSAPs to maintain a proactive cyber posture.

For more information on this and other cybersecurity initiatives, contact ng911wg@cisa.dhs.gov or visit cisa.gov/safecom/next-generation-911 and cisa.gov/communications-resiliency.

# Telephony Denial of Service Attacks: Lessons Learned from a Public Safety Answering Point

## Background

TDoS attacks occur when a large volume of telephone calls overloads a communications network element – overwhelming call capacity and disrupting communications.[1]

Throughout 2020 and 2021, a local public safety answering point (PSAP) responded to daily telephony denial of service (TDoS) attacks impacting operations. To date, these attacks have only impacted the agency's ten-digit non-emergency lines. These numbers are often provided to other agencies, alarm companies, and the public to report non-emergencies.

This case study document highlights the impacts, response, long-term recovery, and the lessons learned from one PSAP's experience with a TDoS attack.

## Impacts

These attacks occur upwards of 12 times per day and are believed to be conducted by foreign actors. The time and number of occurrences vary day-to-day and consume valuable resources, including underlying technology resources and sometimes up to six personnel. During these TDoS attacks, the perpetrator engages a telecommunicator while simultaneously conferencing in additional telecommunicators, resulting in a confusing situation where multiple personnel are on the same call. During these incidents, the telecommunicator often hears ringing or a pre-recorded message. In some instances, the telecommunicator hears audio of a person talking or background noise, making it appear as if the call is from a real person. It is believed that the perpetrator sometimes conferences in other agencies as well. The audio is unclear forcing the telecommunicator to ask questions and stay on the line. During these incidents, multiple telecommunicators are conferenced in on the same call and recognize their co-workers' voices alerting them to the malicious nature of the call.

## Response

Initially, the problem was reported to the agency's system administrator. The system administrator quickly contacted the agency's service provider for voice security to help mitigate the TDoS attacks. The attacks were then reported to the director of the agency, the county's security office, and the information technology (IT) department. Additionally, the PSAP director notified the county's IT department, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and surrounding jurisdictions for awareness. The PSAP also engaged with their

[1] CISA.gov, *Cyber Risks to 911: Telephony Denial of Service*, last accessed December 7, 2021.

Commercial Mobile Radio Service providers to get information on the call characteristics; however, they were unable to track the call or provide additional details.

The PSAP implemented a call authentication system appliance from a network security provider for primary and alternate devices in the path of the ten-digit ingress calls. Incoming primary rate interface circuits come into the building from a demarcation point, and from there, connect to the call handling equipment. The PSAP installed this TDoS mitigation appliance in "front" of the call handling equipment and established rules that inspect ingress calls. When certain characteristics of past attacks are met, the appliance addresses the call and keeps it from being passed into the call handling system so that personnel resources do not need to handle the call.

The PSAP does not have formal cybersecurity training for staff; however, the systems administrator engages with staff and supervisors to make them aware of the call characteristics and security capabilities to mitigate TDoS attacks.

## Long-Term Recovery

The PSAP has not been able to trace the calls but continues to record TDoS incidents to help gather information about call patterns. Additionally, data collection is also assisted by e-mail notifications sent by the service provider to the systems administrator when the mitigation function is enacted.

## Lessons Learned

### Review policies and procedures on handling nuisance calls

Telecommunicators may be first to notice nuisance calls. However, they may be reluctant to disconnect from a 911 call for fear of consequences. Emergency communication centers (ECCs)/PSAPs should review policies and procedures to ensure they address nuisance calls. Agencies should also establish temporary standard operating procedures or guidance for responding to TDoS events. Finally, ECCs/PSAPs should ensure staff are familiar with policies and procedures for addressing nuisance calls.

### Engage with service providers

ECCs/PSAPs should engage with service providers regularly. Service providers may be able to identify signs of an attack and mitigate the damage quickly while ECC/PSAP staff make other notifications and changes to their operations. Additionally, providers may be able to validate authenticity using call information.

### Collaborate with neighboring jurisdictions to establish continuity of operations agreements with other ECCs/PSAPs to provide backup call capabilities during TDoS disruptions

ECCs/PSAPs should build relationships and engage with neighboring agencies to develop agreements and protocols to maintain operations in the event of a TDoS attack where service is disrupted. Larger ECCs/PSAPs may require mutual aid from centers of comparable size for backup call-handling assistance. ECCs/PSAPs should develop agreements and notification protocols with

neighboring jurisdictions to respond to service interruptions and establishing steps for notifying each other of an event to help mitigate consequences. ECCs/PSAPs should also develop plans to notify the public on how to request service in the event of a 911 outage.

## Keep a detailed record of the attacks

ECCs/PSAPs should keep detailed records of attacks or attempts, including dates and times, the frequency, and a summary of the attack. This information can help establish call patterns, which may be valuable for service providers. This may also be helpful for investigative purposes and engaging with federal partners, such as the FBI and CISA.

## Include ten-digit lines when implementing Next Generation 911 systems and security capabilities

TDoS attacks can occur on an agency's ten-digit non-emergency lines and implementing rules for blocking harassing calls may be necessary. ECCs/PSAPs should consider non-emergency lines, in addition to emergency lines, when implementing security capabilities.

## Implement call authentication tools

ECCs/PSAPs should consider call authentication tools or services to screen calls for their validity. These tools can assist with call data verification to avoid overwhelming networks with nefarious calls.

---

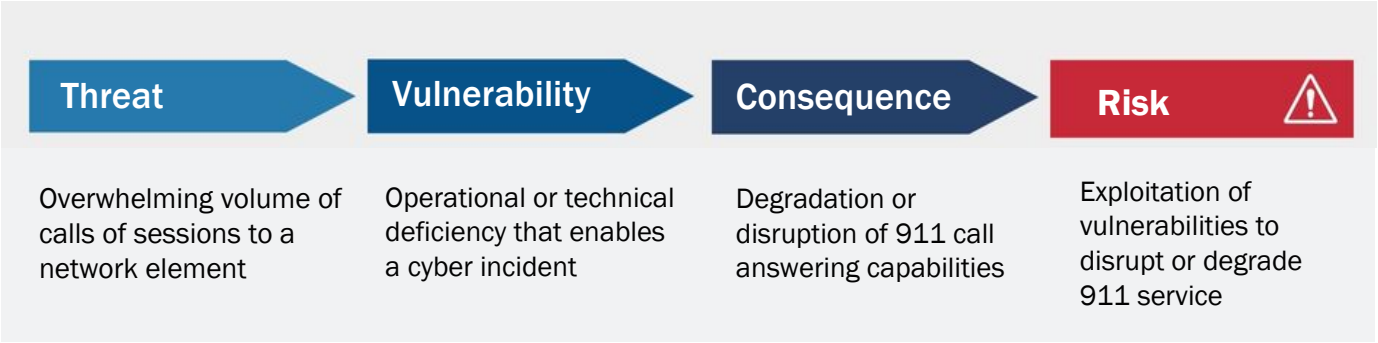
For more information on this and other cybersecurity initiatives, contact ng911wg@cisa.dhs.gov. To learn more about TDoS, visit cisa.gov/publication/next-generation-911 or review the FBI's Private Industry Notice.

# CYBER RISKS TO 911

## TELEPHONY DENIAL OF SERVICE

Telephony Denial of Service (TDoS) events occur when a large volume of telephone calls overloads a communications network element—overwhelming call capacity and disrupting communications. Congestion may occur in any part of a communications network, from the telecommunications provider infrastructure to end-user equipment. Whether malicious (e.g., cyber attack) or accidental (e.g., malfunctioning equipment), TDoS events present a unique challenge for public safety stakeholders, specifically emergency communications centers (ECCs)/public safety answering points (PSAPs). This risk, as outlined in Figure 1, can result in disruptions to call answering capabilities and severely impede a jurisdiction's ability to provide emergency response services.

***Figure 1: Public Safety Communications TDoS Risk***




## TDoS EVENTS

TDoS events can originate from both mobile and fixed-line voice communications systems. Malicious actors may employ a variety of tools to launch TDoS events, including mobile phones, botnets, Voice over Internet Protocol (VoIP) services, compromised private branch exchanges (PBXs), or preprogrammed landline phones. Both 911 and the 10-digit numbers served by ECC/PSAPs can suffer TDoS events. Events affecting 911 numbers originate within the PSAP service area, while events affecting the 10-digit numbers can originate from anywhere. Using this document, ECC/PSAP administrators may familiarize themselves with common TDoS events vectors and best practices to protect networks.

## MOBILE PHONES AND BOTNETS

Mobile phones may facilitate TDoS events, commonly using non-subscriber phones or mobile robot networks, known as botnets. All mobile service providers must connect 911 calls, even if a phone is disconnected from cellular service (i.e. non-subscriber). Non-subscriber mobile phones may not provide detailed identifying or location information to ECCs/PSAPs, obscuring the origin of calls. Large numbers of inexpensive used or pre-paid phones can enable a TDoS events. A mobile botnet is a network of compromised devices remotely controlled by malicious software. Mobile botnets automate TDoS, enabling malicious actors to continuously dial 911 from many devices. Depending on the number of infected devices, mobile botnets can disrupt call answering capabilities in multiple geographic areas.

### Arizona Mobile Botnet TDoS

In 2017, Arizona authorities sentenced an individual for instigating a TDoS event against Phoenix area ECCs/PSAPs. The individual used social media to distribute malicious software onto unsuspecting users' mobile devices. Infected devices began repeatedly calling 911 without user knowledge, disrupting call capabilities at local ECCs/PSAPs.

## VOICE OVER INTERNET PROTOCOL

VoIP provides telephone service through Internet Protocol (IP) networks (e.g., the Internet). VoIP services often depend on a dedicated phone number for emergency services, providing ECCs/PSAPs with a fixed street address when dialed. The VoIP emergency phone number ensures users connect with their local first responders. Unlike a physical landline connection, VoIP customers can subscribe to phone numbers in any geographic area. A malicious actor may subscribe to phone numbers in different geographic areas to target specific ECCs/PSAPs, obscuring the origin of the event.

Malicious actors may also exploit VoIP services to spoof caller identification services. Caller identification spoofing enables perpetrators to make incoming calls appear to originate from a different number. Malicious actors may use spoofing techniques to make a large volume of incoming calls appear to originate from a trusted number, bypassing cybersecurity controls that may otherwise block suspicious traffic.

## COMPROMISED PRIVATE BRANCH EXCHANGES

Private business telephone switching systems, such as PBXs, may be compromised to automatically dial local ECCs/PSAPs. PBXs may be in a business/government facility or hosted on an IP network, which increases vulnerability to physical tampering, malfunction, or cyber attack. Large PBXs in particular can place a substantial volume of concurrent calls to local ECCs/PSAPs.

## PREPROGRAMMED LANDLINES

Local jurisdictions may require private and non-profit sector organizations to maintain landline phones preprogrammed to call 911 (e.g., elevators, pools). For instance, preprogrammed phones are often publicly accessible with highly variable security and maintenance standards. Malicious actors may physically or electronically tamper with these preprogrammed phones to initiate a TDoS events on a local ECC/PSAP. In addition, poorly maintained devices may malfunction and accidentally flood ECCs/PSAPs with false positive emergency calls.

### Texas Preprogrammed Landline TDoS

In 2017, a preprogrammed landline phone in a Houston- area hotel elevator malfunctioned. The device continuously dialed 911 over a 10-hour period, placing thousands of calls to local ECCs/PSAPs. The large volume of calls disrupted voice communications capabilities, preventing ECCs/PSAPs from receiving legitimate emergency calls. Local public safety officials eventually used call location information to track down and repair the malfunctioning device. While ruled an accident, malicious actors may exploit unsecured devices to initiate TDoS events.

## MITIGATION BEST PRACTICES

The Cybersecurity and Infrastructure Security Agency (CISA) is engaging with ECCs/PSAPs, trade associations, and private-sector partners to tailor cybersecurity solutions and best practices for public safety communications users and system administrators. CISA also partnered with SAFECOM and the National Council of Statewide Interoperability Coordinators to publish the Cyber Risks to Next Generation 911. The report provides an overview of Next Generation 911 systems and best practices, empowering public safety communications partners to improve their cybersecurity posture for 911 systems. Table 1 outlines best practices ECCs/PSAPs may consider adopting to reduce the impact of TDoS threats.

*Table 1: Best Practices to Mitigate TDoS Risk*

| Threat | Best Practices |
|---|---|
| Mobile Phones, Botnets, VoIP, and PBX | Maintain call overflow reserve, adding additional call capacity on an as-needed basis to compensate for increased call volume |
| | Establish continuity of operations agreements with other ECCs/PSAPs to provide backup call capabilities during TDoS disruptions |
| | Consider deployment of a TDoS mitigation solution, which can detect and mitigate call overload on administrative and 911 telephone lines |
| | Coordinate with private-sector partners, such as telecommunications service providers, to prepare for TDoS events, including identifying technical solutions and recovery activities |
| | Implement the National Institute of Standards and Technology Cybersecurity Framework to improve |
| | Conduct cybersecurity assessments, identify capability gaps and vulnerabilities, and determine appropriate cybersecurity standards |
| Preprogrammed Landlines | Engage with community partners to maintain and secure devices, as well as share inventory of preprogrammed landlines with ECCs/PSAPs |

## REPORTING

If your organization is experiencing a TDoS event, *immediately* contact telecommunications service providers and federal partners for assistance. In addition, alert the public and share alternative assistance routes. Table 2 identifies federal organizations for assistance, depending on the incident, as well as reporting guidance for TDoS events.

*Table 2: Federal Resources and Reporting TDoS*

| Federal Partner | Component | When to Report |
|---|---|---|
| CISA | CISA Central | Suspected or confirmed cyber incidents that may impact critical infrastructure and require technical response or mitigation assistance |
| Federal Bureau of Investigation (FBI) | FBI Field Offices | Cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity |
| | Cyber Task Forces | |
| | Law Enforcement Enterprise Portal | |
| United States Secret Service | Secret Service Field Offices | Cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card and other financial payment information |
| | Electronic Crimes Task Forces | |

# "First 48": What to Expect When a Cyber Incident Occurs

*Advice from Public Safety Colleagues*

## Introduction

Public safety communications are at risk from a multitude of cyber threats and vulnerabilities. Due to the urgent nature of the operations, public safety communications are high-value targets for cyber threat actors.

This document, developed in partnership with public safety officials who have first hand experience with cyberattacks, will inform expectations and provide recommendations on how to proceed after experiencing a cyber incident. A cyber incident will jeopardize the confidentiality, integrity, or availability of digital information or information systems. As responses to specific incidents vary greatly, this document will provide foundational guidance on cyber incident response expectations.

Common themes, insights, and best practices from public safety colleague interviews are presented throughout the document as text boxes and visual aids. Appendices link to additional public safety cyber resources. The "First 48" focuses on cyber incidents, but organizations are encouraged to holistically review their operational posture to ensure that they remain resilient in instances of other human-caused or natural disruptions (e.g., device management, dependencies on non-agency infrastructure and services).


Cyberattacks have increasingly targeted public safety organizations, utilizingattacks such as telephony denial of service (TDoS), malware, and ransomware to cause disruptions of critical operations. In some instances, organizations are unaware that they are experiencing a cyberattack until they are informed by outside entities such as the Federal Bureau of Investigation (FBI). In other instances, it is immediately obvious the organization is under attack.

It is key for organizations to develop a "culture of cyber readiness" and work collaboratively with all stakeholders who influence or impact their cyber posture. It is recommended that organizations examine external resources that could assist in protecting their systems and networks from threats, preserving forensic evidence, mitigating incidents, and recovering from disruptions. Resources to develop a culture of cyber readiness are available in Appendix A: Cybersecurity Planning Resources.

Public safety colleagues stress planning and preparing against cyber incidents and vulnerabilities. It is recommended that organizations regularly review and assess their cybersecurity posture. Resources such as CISA's Cyber Essentials Toolkit, Public Safety Communications and Cyber Resiliency Toolkit, and the Cybersecurity Incident and Vulnerability Response Playbooks are available to assist organizations in understanding the fundamentals of cybersecurity and communications resiliency.

In addition to reviewing guidance, organizations must familiarize themselves with existing available cyber support. Whether with jurisdictional partners or state and federal level technical cyber support, it is recommended that organizations establish and maintain a close relationship with these stakeholders and involve them in the planning and preparation processes. Third-party vendors, public information offices, and other impactful stakeholders could also be involved.

## PRE-INCIDENT

### *What to Expect:*

- There are daily cyberattack campaigns against public safety networks; some colleagues have observed eight to 12 campaigns at any given moment against their systems
- It could take 18 months to discover a cyberattack; some malware could dwell on the network from 70 to 200 days before launching the attack
- Often, there are more minor incidents leading to a significant, more damaging incident
- Backups connected to the live production system may be impacted during a cyber incident
- Staff may be unfamiliar with potential signs of a cyber incident
- Staff may unknowingly cause cyber incidents via everyday routines (e.g., checking personal email, accessing the internet at a workstation that is connected to the Computer-Aided Dispatch system)
- Vendors may neglect to perform necessary security upgrades and patching
- Compromise of city or municipal networks effect connected Emergency Services systems. When the city is targeted, the Emergency Services networks are often compromised

### WHEN TO BE SUSPICIOUS

- Activity on unusual network ports
- Alerts from malware or antivirus protection systems
- Attempts from normal users to gain elevated privileges
- A threat from a group stating that a cyberattack is imminent (ransomware)
- Configuration changes that cannot be tracked to known updates
- Repeated system or application crashes
- Unauthorized creation of new user accounts
- Unexpected user account lockouts
- Unexplained browsing to unauthorized websites
- Unexplained modifications or destruction of user files
- Unusual deviation from typical network traffic flows
- Web server log entries that show the usage of a vulnerability scanner

### *Advice from Collegues*

Organizations should develop a cyber incident response plan and ensure that it is reviewed, practiced, and updated on a scheduled basis. In addition, establish an incident communications plan that clearly outlines the chain of command, individual roles and responsibilities, emergency purchasing powers eg., hardware, software, services for recovery), and who to contact if an incident should occur to streamline information sharing via unified messaging.

Organizations may also consider implementing or updating continuity of operations procedures (COOP) to strengthen overall cyber resiliency. In the event of a cyber incident, COOP endures the continuation of critcical services and could potentially lessen the strain on getting these services back online before they are completely restored.

Ensure operating systems and applications are up-to-date and fully patched. Develop and maintain images of servers, workstations, and operating systems with IT department to ensure that backups are stored offline. Consider network segmentation as a physical and virtual mergency communications should operate separately from the municipality administrative network.

Staff with technical knowledge and skills and an understanding of organizational network and system architecture could reduce cyber incidents or expedite incident response time. Other resources such as diagrams and other visual aids could also be helpful. Regularly train all staff to practice good cyber hygiene and frequently exercise operating under manual mode to help prevent, discover, and respond to cyber incidents better.

## THE FIRST EIGHT HOURS

### *What to Expect:*

- Organizations may not be aware that they are being targeted and attacked until an outside organization notifies them (e.g., FBI, neighboring jurisdictional partner, third-party vendor)
- Organizations may be unfamiliar with existing reporting channels and resources available to them; the incident may also cause established communications channels and reporting mechanisms to become unavailable (e.g., Internet/phone unavailable)
- Resources may not be available to organizations at the onset of an incident (e.g., IT department is not available on a 24/7 365 schedule; other incidents of higher precedent consuming national or regional resources; cyber incidents may rank lower on the risk registers, thus not warranting immediate assistance)
- Personnel may be confused as to what occurred and may unknowingly destroy forensic evidence and exacerbate the incident
- Information will change rapidly as new evidence is discovered; it is recommended to establish a point of contact to act as the response coordinator to ensure a continuity of information and response efforts

**EXAMPLE INCIDENT RESPONSE ESSENTIAL ACTIONS**

- Leverage assessments and evaluate mission impacts to prioritize resources and identify which systems must be recovered
- Establish and maintain internal reporting structure
- Block and log unauthorized access
- Change system admin passwords and access
- Direct the cyber threat to a sandbox or another form of containment to monitor the threat's activity, gather additional evidence, and identify attack vectors

### *Advice from Colleagues:*

It is recommended that organizations deploy the cyber incident response plan as soon as they observe signs of compromise. A part of incident response includes contacting relevant local (e.g., organizational leadership, emergency management), state (e.g., state chief information officer, governor), and federal authorities (e.g., FBI field office, CISA) and assembling the incident response team (e.g., municipal IT team, vendors). The incident response team and appropriate resources must work together to isolate affected networks and systems. Removing affected devices from the network in the event of a cyber incident may stop or slow the spread of the incident. However, this step will impact operational continuity, which should be considered in the plan. In the process of removing the devices from the network, do not turn them off as doing so may lose valuable information contained in the flash memory. Attackers will often place items in the flash memory to hide their tracks, turning off affected devices may lose these indicators. It is also crucial to capture and preserve forensic evidence to the greatest extent possible, while ensuring system logs are also available for review. Designate physical and virtual meeting space to conduct and document all response activities.

| Example Contact List |
| --- |
| • Local Leadership and Partners (e.g., Office of Public Information, Budget Office) |
| • State Leadership |
| • Jurisdictional Partners |
| • Federal Partners (e.g., FBI Field Office, CISA) |
| • Additional Partners |

After initial triage and response, organizations should consider implementing the previously established communications plan to keep the public, media, and other peripheral stakeholders informed and updated.

## THE FIRST DAY

### *What to Expect:*

- Organizations may need to procure new devices and machines immediately, which may be outside of the limits of existing budgets or policies
- Forensic evidence associated with the incident may be damaged and crucial information may be lost
- Physical components not directly related to the communications systems may be impacted (e.g., HVAC)
- Staff and external stakeholders may be unaware of the latest decisions and updates, thus becoming doubtful and reluctant, potentially leading to low morale
- External subject matter experts may be unfamiliar with the organization's architecture; they may also be challenged to collaborate if there is not an established chain of authority

**EXAMPLE INCIDENT RESPONSE/RECOVERY ESSENTIAL ACTIONS:**

- Remediate all infected IT environments and reimage all affected systems
- Rebuild hardware
- Replace compromised files with clean versions
- Install patches
- Reset passwords on compromised accounts
- Monitor for signs of adversary responding to containment activities
- Develop response scenarios for threat actors using alternative attack vectors
- Allow adequate time to ensure all systems are clear of all possible cyber threat persistence mechanisms
- Ensure all adversary activity is contained prior to rebuilding and reconnecting to the network; if not contained, adversaries could reinfect the rebuilt system

### *Advice from Colleagues:*

During the first day, it is important to locate any remaining backdoor access to the organization and secure these vulnerabilities to prevent further damage. While removing affected devices from the network, if possible, organizations should simultaneously review and authenticate the integrity of backups. This integrity review is crucial to ensure the network is not reinfected. After the authentication process, apply appropriate backups to unaffected or new machines.

Organizations could consider employing outside organizations with subject matter experts to examine networks and systems to remove the remaining cyber threat. However, outsourcing some or all of the responses could be burdensome based on the organization's size, budget, location, and resources available. In addition, the initial response period may be intense and lengthy, spanning more than 24 hours. Accordingly, organizations may need to implement work shifts to alleviate fatigue, maintain continuous coverage, and manage scarce resources.

Should organizations elect to employ third-party support, ensure that access is granted only to those with "need-to-know." Organizations should review contracts and agreements with third-party support to define data and infrastructure management, security practices, and roles and responsibilities during incident response.

Organizations should continue to communicate and update relevant stakeholders. Some victims are reluctant to notify because they do not want to advertise what happened. Organizations may need to consider if sharing specific incident details judiciously and securely could prevent similar attacks.

## TWO DAYS AND BEYOND

### *What to Expect:*

- Incident response may take more than 48 hours; personnel may become fatigued, and resources strained
- Staff may be unfamiliar with operating in manual mode, causing delays in response and services
- Municipal administrative functions (e.g., timesheet, payroll) may be impacted in addition to public safety operations
- Jurisdictional partners may experience similar incidents or attacks
- There may be pressure from leadership, media, and the public demanding incident details and immediate mitigation solutions

**EXAMPLE INCIDENT RESPONSE/RECOVERY ESSENTIAL ACTIONS:**

- Ensure root cause has been eliminated or mitigated
- Identify infrastructure problems to address
- Identify organizational policy and procedural problems to address
- Review and update roles, responsibilities, interfaces, and authority to ensure clarity
- Identify technical or operational training needs
- Improve tools required to perform protection, detection, analysis, or response actions

### *Advice from Colleagues:*

As the response operation continues, organizations should maintain previously established procedures unless they discover additional issues. For example, if the cyber response has transitioned to cyber recovery, organizations need to maintain strategic coordination to keep bringing sanitized devices and systems back online. If the incident remains in eradication and containment phase, organizations should continue to deploy and manage resources to maintain coverage while avoiding fatigue.

Organizations could also consider conducting a hotwash to discuss initial after-action lessons and insights while the response and recovery process continues. Documentation of crucial observations and findings should include:

- Indicator of compromise
- Adversary tactics, techniques, and procedures
- Log data and technical artifacts
- Indication of additional victims (in cases of malicious cyberattacks)
- Safeguard or mitigation that would prevent a similar incident from occurring in the future

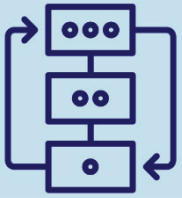
Reviews and discussions of incident artifacts and documentation could impact response and recovery in real-time. In addition, such discussions could assist external investigative organizations, such as the FBI and CISA, to better analyze the incident and develop leads.

## Conclusion

As highlighted in the numerous interviews that helped build the expertise in this document, the preparation before any cyber incident occurs will determine actual response success. Cybersecurity is a shared responsibility; identifying, coordinating, and cementing relationships with all partners will impact the success of the incident response.

## SUMMARY OF RECOMMENDATIONS

Build a culture of cyber readiness



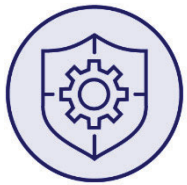
Engage with leadership and review organizational cyber incident response planning

Establish and maintain close relationships and maintain points of contact with cybersecurity partners and involve them in the planning and preparation process, such as:

- Organization leadership and staff
- Network system providers (including internal and external interfaces)
- Identify management adminstrators
- Cyber threat, vulnerability, and intelligence sources
- Entities with potential mission impacts (eg. jurisdictional partners)
- Response, investigate, and recovery resources
- Third-party vendors
- Public information offices

Review cyber resources (Appendix B: Cybersecurity Planning Resources)

Regularly review and assess cybersecurity posture



Holistically review operational posture to remain resilient in instances of non-cyber human-caused or natural disruptions

## Appendix A: Common Cyber Incident Response Pitfalls and Solutions

Below is a list of common cyber incident response pitfalls and corresponding solutions presented throughout the document. Please note the lists are not comprehensive. Organizations are recommended to review guidance, requirements, and relevant legislature to ensure solutions are appropriate and tailored to meet their mission needs.

| THE FIRST 8 HOURS | THE FIRST DAY | TWO DAYS AND BEYOND |
|---|---|---|
| **Pitfall:** Lack of planning and resources | **Pitfall:** Lack of authority and communication | **Pitfall:** Recovery fatigue |
| SOLUTIONS:<br>• Ensure the cyber incident response plan is reviewed, practiced, and updated on a scheduled basis<br>• Deploy the cyber incident response plan as soon as signs of compromise are observed<br>• Contact relevant local, state, and federal authorities<br>• Assemble the incident response team<br>• Remove affected devices from the network<br>• Capture and preserve forensic evidence to the greatest extent possible<br>• Ensure system logs are also available for review<br>• Conduct meetings and document all response activities | SOLUTIONS:<br>• Locate remaining backdoor access to the organization and secure these vulnerabilities<br>• Review and authenticate the integrity of backups; once authenticated, apply appropriate backups to unaffected or new machines<br>• Consider collaborating with outside organizations with the subject matter expertise to examine networks and systems to remove the remaining cyber threat<br>• Implement work shifts to alleviate fatigue and maintain continuous coverage<br>• Communicate and keep stakeholders, leadership, the public, and the media informed | SOLUTIONS:<br>• Maintain previously established procedures unless additional issues are discovered<br>• Maintain strategic coordination to continue to bring sanitized devices and systems back online<br>• Conduct a hotwash to discuss initial after-action lessons and insights while the response and recovery process continues |

## Appendix B: Cybersecurity Planning Resources

- Public Safety Communications and Cyber Resiliency Toolkit: An interactive directory of resources that assist public safety agencies and others responsible for communications networks in evaluating current resiliency capabilities, identifying ways to improve resiliency, and developing plans for mitigating the effects of potential resiliency threats.
- Cyber Resiliency Resources for Public Safety Fact Sheet: A compilation of cyber resiliency assessment tools and programs provided by the federal government, industry, and trade associations designed to assist agencies in taking proactive measures to enhance their overall cybersecurity posture.
- Guide to Getting Started with a Cyber Risk Assessment: Public safety organizations may use this customizable guide to learn about and document organizational networks, components, risk levels, and vulnerabilities.
- Cyber Essentials: A guide for leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices. The Cyber Essentials Starter Kit contains the basics for building a culture of cyber readiness
- Federal Government Cybersecurity Incident and Vulnerability Response Playbooks: Operational procedures for planning and conducting cybersecurity incident and vulnerability response activities in Federal Civilian Executive Branch (FCEB) Information Systems that can also be used by critical infrastructure entities; state, local, territorial, and tribal government organizations ; and private sector organizations to benchmark their vunerability and incident response practices. The playbooks provide illustrated decision trees and detail each step for both incident and vulnerability response.
- CISA Interoperable Communications Technical Assistance Program (ICTAP): The ICTAP serves all 56 states and territories and provides direct support to state, local, and tribal government officials through the development and delivery of training tools, and onsite assistance to advance public safety interoperable communications capabilities. Example public safety communications resiliency-specific services include public safety answering point cyber awareness webinar, Statewide Communication Interoperability Plan workshop, Next Generation 911 strategic planning, and other cybersecurity technical assistance offerings.
- Incident Response Training: CISA offers a no-cost cybersecurity incident response training for government employees and contractors across federal, state, local, tribal, and territorial government, and is also open to educational and critical infrastructure partners.
- Detection and Prevention: CISA rapidly notifies relevant critical infrastructure stakeholders of elevated risk exposure, conducts incident management operations, provides vulnerability assessments, and directly deploys risk management information, tools, and technical services to mitigate risk, including regulatory enforcement where authorized.
- Subscribe to Cybersecurity and Infrastructure Security Agency (CISA) Alerts: Sign up to receive CISA-curated alerts and notifications.
- Report Cyber Issue: Report incidents, phishing attempts, malware, and vulnerabilities through CISA's secure mechanism.
- CISA's Cyber Hygiene Vulnerability Scanning: Register for this service by emailing vulnerability@cisa.dhs.gov. Once initiated, this service is mostly automated and requires little direct interaction CISA performs the vulnerability scans and delivers a weekly report. After CISA receives the required paperwork, scanning will start within 3 business days, and organizations will begin receiving reports within two weeks.
- Get your Stuff Off Search (S.O.S.): While zero-day attacks draw the most attention, frequently, less complex exposures to both cyber and physical security are missed. Get your Stuff Off Search–S.O.S.–and reduce internet attack surfaces that are visible to anyone on web-based search platforms.

## ADDITIONAL ONLINE RESOURCES & TOOLS

**PUBLIC SAFETY CYBERSECURITY | CISA:** This page compiles resources developed by CISA for public safety communications practitioners, as well as anyone looking to gain further knowledge about cybersecurity for public safety communications. This page provides resources to public safety practitioners regarding common questions related to public safety cybersecurity.

**RELEASES · CISAGOV/CSET (GITHUB.COM):** The Cyber Security Evaluation Tool (CSET®) is a stand-alone desktop application that guides asset owners and operators through a systematic process of evaluating Operational Technology and Information Technology. After completing the evaluation, the organization will receive reports that present the assessment results in both a summarized and detailed manner. The organization will be able to manipulate and filter content in order to analyze findings with varying degrees of granularity. It includes the Cyber Resilience Review and Cyber Infrastructure Survey.

On June 30, 2022, CISA Current Activity announced that CSET now includes a new module: Ransomware Readiness Assessment (RRA). The RRA is a self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident; completing the RRA is recommended.

**TRANSITION TO NEXT GENERATION 911 (NG911) | CISA:** CISA, in conjunction with the SAFECOM-NCSWIC Next Generation 911 (NG911) Working Group, uses stakeholder feedback from multiple levels of government to identify, document, and develop informational products and refine innovative concepts that will facilitate the transition to NG911. This page provides resources and tools to support 911 system operations, security, and NG911 transition.

**CYBERSECURITY | 911.GOV:** The National 911 Program continues to collaborate with the 911 community and other federal agencies to provide support for the development of cybersecurity resources. The Program's Documents & Tools section includes specific resources aimed at increasing understanding of cybersecurity issues and reducing the threat to emergency communications.

**CYBER RESOURCE HUB | CISA:** The Cybersecurity and Infrastructure Security Agency offers a range of cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust and resilient cyber framework. These professional, no-cost assessments are provided upon request on a voluntary basis and can help any organization with managing risk and strengthening the cybersecurity of our Nation's critical infrastructure.

**NEXT GENERATION 911 SELF-ASSESSMENT TOOL | 911.GOV:** The SAFECOM National Council of Statewide Interoperability Coordinators (NCSWIC) NG911 Working Group commenced work on the development of a dynamic NG911 Self-Assessment Tool for use by state, regional and local PSAP and emergency communication center leadership.

Download the NG911 Self-Assessment Tool