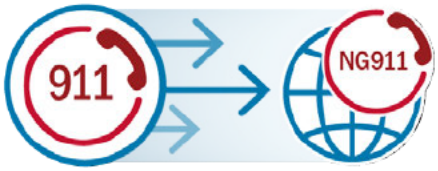
Considerations for Cyber Disruptions in an Evolving 911 Environment

Next Generation 911 Capabilities



The increased interconnectivity of Next Generation 911 (NG911) systems exposes new vectors for threats that can disrupt or disable the operations of emergency communications centers (ECCs).[1] The disruptions may cause call backlogs and delayed response to emergencies or the transfer of operations to manual mode or alternate ECCs.[2] Federal, state, local, tribal, and territorial agencies are making some progress transitioning to NG911. NG911 presents opportunities to enhance the resilience of 911 systems. However, ECCs may still face disruptions of services even with robust cybersecurity practices.[3] ECCs may have the capability to transfer calls to a neighboring center or a center farther away for processing during or after an attack, even though personnel may not be required to physically evacuate the centers.

A cybersecurity incident can be caused by a multitude of factors. For example, disruption of service can be caused by malicious actors seeking to delay critical, life-saving services or it can also result from an errant software update to a managed service provider's network.

To better prepare for disruptions in ECCs, this document identifies examples of cybersecurity vulnerabilities and threats that can impact 911 systems (Figure 1: Example Risks to NG911 System Components). It also provides ECCs with considerations for engaging with partners to establish, update, and maintain Continuity of Operations (COOP) plans to better prepare for cyber disruption events in an evolving 911 environment.

User and Devices	Network Infrastructure and Connections	Data, Applications and Services
• Data Breaches • Insider Threats • Malware • Ransomware • Spear-Phishing • Spoofing	• Denial-of-Service Attack • Man-in-the-Middle Attack • Telephony-Denial-of-Service Attack • Unauthorized Network Access	• Malicious Applications • Swatting • Unauthorized Data Access • Ransomware Encryption • Ransomware Exfiltration • Denial-of-Service

Figure 1: Example Risks to NG911 System Components

[1] These centers include ECCs, public safety answering points, public safety communications centers, emergency operations centers, and other public service communications centers.
[2] "Alternate ECCs" include backup centers where calls and operations may be transferred following disruptions of service.
[3] For more resources on cyber risks to NG911, visit CISA's Transition to NG911 webpage.

COOP Benefits and Development

Establishing a COOP plan can help ensure the continuity of critical services during a cyber disruption event while services are being restored. A COOP plan includes the actions staff members must take to ensure employee and facility safety and accountability. Without this essential planning—followed by provisioning and implementing continuity principles in a NG911 environment—first responders may be unable to provide services to help citizens when needed the most.

When beginning to build a COOP plan, an organization should consider reviewing existing state and local continuity resources and regulations. Additionally, the Federal Emergency Management Agency's (FEMA) brochure—*What is Continuity of Operations?*—highlights overarching continuity requirements and phases of COOP activation for agencies.

Updating a COOP Plan for NG911

ECCs may be unable to maintain operations following a cyberattack that causes the network or even utility services for the center to fail. Dependency on third-party infrastructure can also introduce vulnerabilities.[4] ECCs may need to identify an alternate center in which their personnel can perform operations or route calls to during outages and disruptions of service. With the transition to NG911, the COOP plan should be updated to outline any emergency services required to meet their mission and alert the affected public safety agencies, field personnel, stakeholders, and the public of the lost access to 911.

The following is a checklist of considerations for updating COOP plans and is intended to help ECCs ensure continuity of operations with NG911 systems during cyber disruptions:

CONSIDERATIONS FOR UPDATING COOP PLANS
Collaborate with Personnel, IT, Stakeholders, and Partners to Identify Alternate ECCs
☑ Determine infrastructure, resources, and personnel critical for optimal response, coordination, and communication during outages to activate the COOP plan
☑ Establish mutual aid agreements and memoranda of understanding with relevant partner agencies involved in processing or transferring calls during cyber incidents
☑ Communicate and inform the alternate ECC about the affected primary ECC and expectations involved with the transfer of operations *(NOTE: All public safety agencies involved should be aware of the call volume, staffing, cross-border data transfer availability, performance measures, and recovery issues before deciding on an alternate ECC)*.[5]
☑ Outline steps for restoring and transferring calls from the alternate ECC to resume normal operations at the affected ECC
☑ Ensure COOP plans and critical contact information are accessible offline in the event of a cyber disruption

[4] ECCs can find more information about ensuring continuity of operations while using third-party dependencies in Public Safety Communications Dependencies on Non-Agency Infrastructure and Services.
[5] Some state laws may not allow for cross-border data transfer.

Establish Protocols for Maintaining Data

- Establish protocols for maintaining data and responsibilities to establish who owns the data, how it should be maintained and stored when at rest and transit, and the costs associated with transferring and storing data
- Test the ability to restore systems from backups and assess the process with IT and cybersecurity specialists
- Consider mandatory backup of data on a secondary drive that is stored offline to ensure further separation and security

Engage with Partners and Stakeholders

- Establish notification plans to inform all field personnel, public safety agencies, stakeholders, and the public once normal operations are restored or notify them of an extended outage
- Notify and coordinate with partner agencies and stakeholders to discuss their envisioned role in the ECC's COOP plan; give time to collaborate, discuss, and agree on roles and responsibilities defined in the COOP plan
- Engage the private sector such as service providers (internet, power, telecommunications, and commercial mobile radio service) and the Public Information Office (PIO) or media to ensure all partners are aware of roles and responsibilities in restoring operations

Address Cybersecurity Risks to NG911 Systems

- Develop cyber incident and vulnerability response plans to ensure minimal gaps in service
- Explore the SAFECOM Transition to NG911 webpage for resources for ECCs and stakeholders to access cybersecurity best practices and case studies
- Consider contacting the local Cybersecurity and Infrastructure Security Agency (CISA) Cyber Security Advisor or Emergency Communications Coordinator, or CISA Central for technical assistance opportunities, such as resources from the Interoperable Communications Technical Assistance Program (ICTAP), including the ICTAP Service Offerings Guide and CISA's Technical Assistance Request Form

Establish a COOP Planning Cycle

- Develop training and exercises to replicate both normal and heightened conditions to test systems, protocols, and personnel. Include information regarding service providers and points of contact following cyber disruptions, as well as recovery processes for backups and restoration of normal operations
- Pre-plan drills and tabletop exercises to ensure or reduce disruptions to essential functions and critical services during an emergency or cyber disruption

Appendix: Resources for COOP Planning

RESOURCE	DESCRIPTION
Association of Public-Safety Communications Officials (APCO) - International	
APCO Continuing Dispatch Education Course: Disaster Operations and the Communications Center	This training offers information for telecommunications emergency management professionals and provides guidance on continuity of operations for the communications center in the face of a multitude of disaster situations.
Managing Operational Overload in the Emergency Communications Center	This standard seeks to serve as a guiding document to assist ECC staff in their efforts to prepare for a multitude of events as they create pre-planning and mitigation documents.
CISA	
National Emergency Communications Plan (NECP)	The NECP is the Nation's strategic plan to strengthen and enhance emergency communications capabilities.
Transition to NG911	This webpage offers a vast array of resources and tools to support 911 systems operations, security, and NG911 transition.
Cybersecurity Incident & Vulnerabilities Response Playbooks	These playbooks are a standard set of procedures for Federal Civilian Executive Branch agencies to identify, coordinate, remediate, recover, and track successful mitigations from incidents and vulnerabilities affecting their IT systems, data, and networks.
Emergency Services Sector Continuity Planning Suite	This resource provides a centralized collection of existing guidance, processes, products, tools, and best practices to support the development and maturation of continuity planning for the first responder community.
First 48: What to Expect When a Cyber Incident Occurs	This document highlights helpful steps in the first 48 hours following a cyberattack, including advice from public safety colleagues.
FEMA	
2018 Continuity Guidance Circular	This document serves as a resource to guide, update, and maintain organizational continuity planning efforts.
Continuity Assessment Tool	This interactive tool can be used to identify shortfalls or gaps in an organization's continuity planning.
National Emergency Number Association	
Continuity of Operations Plans for PSAPs	This training provides guidance on writing comprehensive and effective COOP plans, as well as strategies for informing and educating team members and methods for enacting plans under extreme circumstances.
NG911 Transition Planning Considerations	This document provides ECCs with information to consider in preparation for the transition to NG911, including four use cases based on the transition status of the originating or terminating entity.
National 911 Program Office	
911 Cybersecurity	This webpage provides documents, tools, and resources for the 911 community.
State of Connecticut	
Cyber Disruption Response Plan	This document offers an example framework for a cyber disruption plan, including response and recovery recommendations.