Nebraska Public Service Commission

Public Safety Answering Point
Continuity of Operations Planning
Education Guide

July 2021

OVERVIEW

This Continuity of Operations (COOP) Planning Education Guide is intended to be used in conjunction with the COOP Planning outline to assist Nebraska 911 Public Safety Answering Point (PSAP) and Emergency Communications Center (ECC) managers in the preparation of a specific COOP plan that meets the needs and circumstances of their agencies and jurisdictions.

This guide was developed in conformance with COOP planning methodologies promulgated by the Federal Emergency Management Agency (FEMA), the National Fire Protection Association (NFPA), and the National Emergency Number Association (NENA).

Additional COOP planning guidance is available online at the following websites:

FEMA: Federal Continuity Directive 1 *Federal Executive Branch National Continuity Program and Requirements*, January 17, 2017

https://www.fema.gov/sites/default/files/2020-07/January2017FCD1.pdf

FEMA: Federal Continuity Directive 2 *Federal Executive Branch Mission Essential Functions and Candidate Mission Essential Functions Identification and Submission Process*, June 13, 2017

https://www.fema.gov/sites/default/files/2020-07/fema_federal-continuity-directive-2_061317.pdf

NFPA 1600: *Standard on Continuity, Emergency, and Crisis Management*, 2019

https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600

NENA-INF-017.3-2018: *NENA Communications Center/PSAP Disaster and Contingency Plans Model Recommendation*

https://www.nena.org/resource/resmgr/standards/nena-inf-017.3-2018_disaster.pdf

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose

Continuity is defined as *the ability to provide uninterrupted services and support, while maintaining organizational viability before, during, and after an event that disrupts normal operations.*[1] A COOP plan is a tool that is intended to aid an organization in preparing for, responding to, and recovering from a disruptive event.

The purpose of a PSAP COOP Plan is to protect the PSAP's 911 system, prevent disruptions from occurring, mitigate the impact of unplanned disruptions, and quickly recover when a disruptive event occurs. The personnel, facilities, equipment, infrastructure, and applications that support the 911 system are susceptible to a variety of risks. These include natural and technological hazards and threats posed by intentional acts. In addition, modern 911 networks and systems that support public safety agencies are vulnerable to cybersecurity threats.

1.2 Applicability and Scope

The nation's emergency services and public safety organizations have been designated as a *critical infrastructure sector* by the Department of Homeland Security (DHS).[2] Critical infrastructure is defined as "*systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*"[3]

Public Safety Telecommunicators (PSTs) as "911 center employees" are classified as *essential critical infrastructure workers* by the DHS Critical Infrastructure and Cybersecurity Agency (CISA).[4] Individuals serving in a public safety position in law enforcement, fire/rescue, emergency medical services (EMS), and emergency management are designated as essential critical infrastructure workers. The work performed by PSTs is critical to the health and safety of the community and must continue during disruptive events.

A PSAP COOP Plan describes how the PSAP will sustain the capability to perform critical functions during and after a disruption of internal operations—whether caused by natural disasters, technology failures, or malicious incidents. Key objectives to be accomplished by the adoption of a COOP Plan include:

- Minimize disruption to normal service levels
- Mitigate the extent of disruptive events and damage
- Minimize fiscal impacts of disruptive events
- Prepare personnel to implement emergency procedures
- Establish an alternate method to continue service delivery
- Provide for the rapid and efficient restoration of services

---

[1] *Federal Continuity Directive 1 (FCD-1)*. U.S. Dept. of Homeland Security (DHS), January 2017

[2] Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection

[3] 42 U.S. Code § 5195c. Critical infrastructures protection

[4] Memorandum on Identification of Essential Critical Infrastructure Workers during COVID-19 Response. (CISA), March 19, 2020

The PSAP COOP Plan presents a continuity strategy to assure the resilience and operational capacity of the PSAP. Resilience is defined as *the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions ... [it] includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents*.[5]

A COOP Plan encompasses all phases of the continuity management process and outlines the steps necessary for the PSAP to maintain operational capacity during a localized or region-wide disruption of normal operations. The disaster and continuity planning process include four distinct yet overlapping phases:

Prevention – Activities that are implemented before an emergency occurs to avert or minimize the probability of occurrence and the related potential impact of a given hazard.

Preparedness – Activities that are intended to enhance the capacity of an organization to protect itself from the effects of emergency events. Preparedness activities include developing response plans, maintaining situational awareness, acquiring protective equipment, training staff, and conducting drills and exercises.

Response – Activities that are initiated to address the immediate effects of an emergency through the application of procedures and emergency resources. These activities are intended to protect lives and property and meet short-term human needs.

Recovery – Activities that involve both short- and long-term actions that are intended to restore the operational capacity to a pre-disaster condition.

1.3 Planning Concepts

A systematic approach to continuity planning involves activities across each phase of the continuity cycle. An effective continuity program is responsive to known, emerging, and immediate threats. Examples of continuity planning activities include:

- Identifying the hazards and threats that may impact the 911 facility and system infrastructure
- Maintaining situational awareness of emerging threats
- Preparing response procedures to assure the continuity of essential services
- Providing training for personnel regarding COOP Plan activation
- Coordinating continuity activities with partner agencies and contractors
- Developing agreements with external partners and contractors to provide support services during a disruptive event
- Activating continuity procedures in response to developing or sudden events
- Managing post-incident disaster recovery activities

[5] "Presidential Policy Directive (PPD)-21 – Critical Infrastructure Security and Resilience" The White House President Barack Obama. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

1.4 Authorities

The PSAP 911 system is managed in accordance with various state regulations, professional standards, and practices promulgated by professional organizations including:

- The Nebraska Emergency Management Act, Neb. Rev. Stat. §§ 81-829.36 to 81-829.75
- 911 Service System Act, Act, Neb. Rev. Stat. §§ 86-1001 to 86-1029.03
- Emergency Telephone Communications Systems Act, Neb. Rev. Stat. §§ 86-420 to 86-441.01
- Enhanced Wireless 911 Services Act, Neb. Rev. Stat. §§ 86-442 to 86-470
- Interlocal Agreement for E911 Public Safety Answering Point Services
- Association of Public-Safety Communications Officials (APCO) International
- National Emergency Number Association (NENA)
- National Fire Protection Association (NFPA)

See Appendix G for a complete list of authorities and references.

1.5 Acronyms and Glossary

See Appendix H for an explanation of acronyms and Appendix I for a glossary of terms that appear in this plan.

2. SITUATION AND ASSUMPTIONS

2.1 Situation

A PSAP is susceptible to a wide range of natural and technological hazards and human-induced threats. It is responsible for assuring the resilience and operational capability of the 911 system regardless of emergency or disaster circumstances. The PSAP is an integral component of the region's public safety infrastructure that may best be described as a system of systems. The system includes telecommunication service providers, network operating centers, voice and data networks, aerial and underground cables, microwave transmission equipment, and PSAPs.

2.2 Assumptions

A COOP Plan is developed based upon the following assumptions:

- The PSAP is susceptible to a wide range of natural hazards, technological hazards, and human-induced threats.
- External and internal emergency incidents that can affect the operational capacity of the PSAP can occur at any time, with little or no warning.
- The PSAP can provide a depth of staffing in key positions that will be sufficient to provide for the continuity of essential services.
- Surrounding PSAPs have adopted COOP plans to address local disruption of services in coordination with your PSAP.
- An alternate worksite (AWS) will be available in the event the main PSAP facility is not accessible or cannot be occupied.

- Contractors that support PSAP network operations have adopted and tested business continuity plans to assure their ability to provide essential services during a large-scale event.

2.3 Risk and Vulnerability Assessment

A risk is a probable threat to an organization that has the potential to cause harm. Vulnerability may best be described as an exposure to risk and its associated consequences. Risk management is the *process of identifying, analyzing, and communicating risk, and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken*."[6] A PSAP seeks to manage risk by implementing controls to mitigate risk and minimize the disruption of normal operations.

2.3.1 Hazards and Threats

A natural hazard is defined as a *source of harm or difficulty created by a meteorological, environmental, or geological phenomenon or combination of phenomena*.[7] A PSAP is susceptible to a range of natural hazards including severe thunderstorms, tornados, flooding, extreme heat, winter storms, and viral pathogens resulting from a pandemic.

Technological hazards are those that result from interactions with the man-made environment such as transportation systems, utilities, communication systems, and hazardous materials.

Human-induced threats involve intentional acts such as violence, attacks on critical infrastructure, terrorism, civil unrest, and cybersecurity attacks.

Communication facilities are susceptible to localized or site-based incidents that can disrupt the operation of departments. These include extended power outages, utility system failures, fires, information technology (IT) network outages, and telecommunication system failures. The PSAP must be prepared to implement continuity procedures to maintain operational capacity regardless of the initiating incident.

The table below presents hazards and threats that may impact public safety communication facilities across Nebraska.

Table 1: Hazards and Threats Matrix

Hazard or Threat	Probability of Occurrence	Estimated Impact Upon Health & Safety			Estimated Impact Upon Operations		
		Limited	*Moderate*	*Major*	*Limited*	*Moderate*	*Major*
Natural Hazards							
Severe Thunderstorm	High	✓				✓	
Tornado	High		✓			✓	

[6] U.S. Department of Homeland Security, *DHS Risk Lexicon,* 2010 Edition, September 2010, pg. 30.
[7] Ibid, page 21.

Hazard or Threat	Probability of Occurrence	Estimated Impact Upon Health & Safety			Estimated Impact Upon Operations		
		Limited	*Moderate*	*Major*	*Limited*	*Moderate*	*Major*
Winter Storm	High	✓			✓		
Extreme Heat	Moderate	✓			✓		
Flooding	High		✓			✓	
Earthquake	Low	✓			✓		
Pandemic Disease	Moderate			✓			✓
Technological Hazards							
Energy Utility Failure	Low	✓					✓
Water Utility Failure	Low		✓			✓	
Computer Network Outage	Moderate	✓					✓
Communication Network Failure	Low	✓					✓
Structure Fire	Moderate		✓				✓
Hazardous Materials Release (Fixed site)	Low	✓			✓		
Hazardous Materials Release (Transit)	Low		✓		✓		
Human-induced Hazards							
Workplace Violence	Low			✓			✓
Cyber (Data/Infrastructure)	Moderate	✓					✓
Sabotage	Low	✓					✓
Civil Unrest	Low	✓			✓		
Terrorism (CBRNE)*	Low			✓			✓
**Chemical, Biological, Radiological, Nuclear, Explosive*							

2.4 Operational Impacts

It is difficult to predict the potential magnitude of a disruption associated with each hazard or threat. Operational impacts may result in damage to a PSAP's facility, destruction of critical network infrastructure, or staff reductions during a pandemic event.

Risk can be categorized in terms of overall impact. They include the loss of physical assets, damage to property, and staffing gaps. Qualitative impacts include harm to the organization's reputation, loss of public confidence in the 911 system, and decreased employee morale. One method to assess potential operational impact is based on the duration of a disruptive event. The duration of a disruptive event is typically described in general terms including:

- **Short-term.** Example: Loss of power to a facility for less than 24 hours
- **Long-term.** Example: The facility sustains damage caused by a tornado
- **Localized.** Example: A hazardous material incident forces evacuation of the facility
- **Regional.** Example: Severe flooding impacts multiple communities and transportation routes within the region
  Pandemic. Example: A pandemic disease event results in the loss of key personnel (See Appendix J for a pandemic disease response plan template)

2.5 Risk Impact

The purpose of identifying risk is to help identify the impacts, continuity strategies, and mitigation steps. A risk matrix can be used to prioritize risk in terms of its likelihood and impact estimates (see Figure 1).

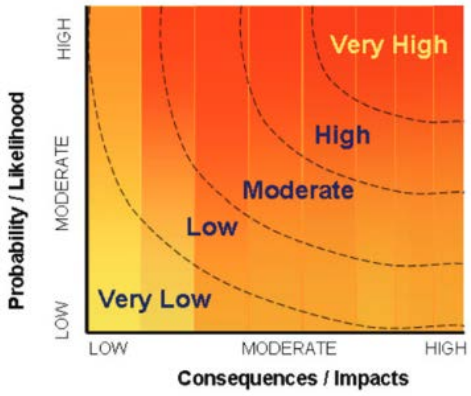

Figure 1: Risk-Rating Matrix Example[8]

As you examine and document the hazards and threats most likely to occur in your region, consider the operational impacts and processes that may change under limited, moderate, or major events. For example, during a limited/low-risk event, PSAP personnel may remain at their current location and operational processes remain static with the team on high alert for changing conditions. If the event is moderate or major, PSAP operations may utilize a backup site, mobile command center, or transfer calls to a neighboring PSAP.

[8] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-mngmnt-pnnng/mrgnc-mngmnt-pnnng-eng.pdf

The figure below presents an example of the failover/rollover operational scenarios in a PSAP with their corresponding risk rating.

Failover Operations Example					
Scenario	**Risk Rating**	**Location of Operations**	**Call Routing Protocol**	**Operational Protocols**	**Notes**
High volume of 911 calls	Low	TCs remain in place	Overflow calls are rerouted to [PSAP NAME]	Callers are transferred back to the PSAP via an administrative line for dispatch	
911 lines are down but radios are fully functioning	Moderate	TCs remain in place	Calls are rerouted to [PSAP NAME]	Callers are transferred back to the PSAP via an administrative line for dispatch	
Radios are down but 911 lines are fully functioning	Moderate	TCs remain in place	911 calls continue to route to PSAP	911 calls are dispatched to first responders via CAD and administrative phone lines	Notification to field responders; establish communications method (e.g., alternate radio frequency, CAD-to-CAD, administrative phone line, cellular phone line).
911 lines and radios are both down	Very High	TCs report to [PSAP NAME]	911 calls are rerouted to [PSAP NAME]	911 calls are dispatched to field responders via [radio, administrative lines, cellular phone] or CAD-to-CAD; TCs report to [PSAP NAME].	TCs grab the bugout bag. Notification to field responders; establish communications method (e.g., alternate radio frequency, CAD-to-CAD, administrative phone line, cellular phone line). Notify staff where to report. Activate GETS and WPS.
911 lines and radios are fully functioning but the building is evacuated	High	TCs report to [PSAP NAME].	911 calls are rerouted to [PSAP NAME]	911 calls are dispatched to field responders via administrative lines or CAD-to-CAD	TCs grab the bugout bag if possible. Notification to field responders; establish communications method (e.g., alternate radio frequency, CAD-to-CAD, administrative phone line, cellular phone line). Notify staff where to report.
Return to normal operations	Normal	TCs report back [PSAP NAME]	911 calls are routed to PSAP	Dispatch protocols return to normal	

Figure 2: Failover/Rollover Operations

2.6 Risk Controls

Vulnerability is reduced through the implementation of prevention measures or controls. Also referred to as mitigation, prevention measures may be in the form of a process, physical device, policy, or procedure. A deterrent is a control or countermeasure intended to discourage, complicate, or delay an adversary's action. Controls are categorized as being either physical or procedural.

Physical Controls are tangible or environmental features and include:

- Access control locks, surveillance systems, fencing, and identification badges
- Law enforcement or security personnel
- Access point alarms, fire-suppression systems, and smoke detection systems
- IT network-monitoring systems
- Uninterruptible power supply (UPS) systems and generators

Procedural Controls are behavior-based and include:

- Personnel hiring policies
- Personnel background screening
- Network access rights
- Password management
- Network monitoring procedures

3. CONCEPT OF OPERATIONS

3.1 General

A PSAP COOP Plan is intended to promote the continuation of services during a disruptive incident or large-scale emergency. The objectives of the COOP Plan include:

- Preserving the public's confidence in the local 911 system
- Protecting the health and safety of agency personnel and visitors
- Enhancing organizational and operational resilience to hazards and threats
- Minimizing the impact on the operational capacity of the PSAP
- Implementing the rapid restoration of essential functions and technology systems

During a continuity event or emergency, PSAP personnel will function within the normal organizational structure and chain of command. PSAP personnel also may be invited to participate in or coordinate with operations of local and regional emergency operations centers (EOCs) during a disaster.

3.2 Mission Essential Functions

A mission essential function (MEF) is a function or task that must be continued throughout, or resumed immediately after, a disruptive event to maintain mission-critical services. Most functions or tasks assigned to PSAP staff are considered MEFs. During a disruptive event, each MEF will be assigned to the primary or an alternate staff member in accordance with the staffing succession procedures. An example is shown below.

Table 2: Mission Essential Function

Mission Essential Function	
Priority	**Functions**
1	
2	

3.3 Mission Essential Workforce

Essential workforce positions are those that are responsible for supporting MEFs or are assigned a critical response role during an emergency incident. Personnel may be required to work extended shifts to assure coverage of positions.

A PSAP manager/director designates the positions and functions that are considered essential to the continuity of services during an emergency event. A PSAP COOP Plan will contain a copy of the organizational chart that details the positions that support the PSAP.

3.4 Succession and Delegation of Authority

Certain positions are essential to the continued operations of the PSAP and must be filled regardless of the emergency circumstances. The guidelines below provide for the orderly succession of authority if the primary individual in a position is unavailable or incapacitated.

Each key position within the PSAP is staffed by an individual on a full-time basis. Some individual staff members may be unavailable during an emergency. Alternate positions must be identified that will assume the duties of each key position. All organizations should strive to designate two or three alternate personnel for each key position. It is assumed that the authorities granted to each key position will transfer to the individuals assigned to serve as an alternate. However, certain authorities may be reassigned to alternate positions. Those serving in an alternate capacity must be properly trained and prepared to support alternate roles and tasks.

MEFs must be maintained. This may require employees to be assigned work of a lower or higher-level classification due to a high level of absences. Supervisors will track the shifts and level of work performed during an incident. Records must be kept on the time that each employee works in each position as well as all overtime and any other receipts for items purchased during the event for FEMA grant reimbursement

Tables that describe the Orders of Succession and Delegations of Authority can be found in Appendix A.

3.5 Essential Systems and Software Applications

PSAP operations are heavily dependent upon a variety of technology systems. Efficient dispatch services utilize electronic systems including 911 call-handling equipment (CHE), computer-aided

dispatch (CAD), records management system (RMS), logging/recording system, geographic information system (GIS), and others. A disruptive event may render these systems inoperable or inaccessible. Hardware and software applications must be documented to support recovery operations.

Tables that document the computer hardware, software applications, data, and records that are essential to PSAP operations can be found in Appendix B.

3.6 Alternative Worksite

A continuity event such as a fire or tornado may damage the PSAP facility making it inaccessible or unusable. Such an event will require the transfer of operations and relocation of personnel to an AWS. The PSAP manager, or their designee, is responsible for determining if the facility is safe to access and equipment suitable for use.

The PSAP should consider the following when selecting the site for an AWS:

- Staff workspace requirements
- Cost and availability of an AWS
- Distance to the AWS
- Time needed to prepare or activate the site for operation
- Transportation of personnel to the AWS
- Equipment and supplies necessary to operate the AWS
- Security and access to the AWS

Informational tables for AWS activation can be found in Appendix C. When considering the information to include, levels of AWS readiness are defined as follows:

Hot Site. An alternate facility that already has in place computers, telecommunications, and environmental infrastructure that is necessary to quickly recover critical business functions or information systems.

Warm Site. An alternate facility that is equipped with minimal computer hardware, communications interfaces, and electrical and environmental conditioning, and which is only capable of providing backup after additional provisioning, installation of software, or customization is performed.

Cold Site. An alternate facility that already has in place the environmental infrastructure required to recover critical business functions or information systems, but does not have pre-installed computer hardware, telecommunications equipment, communication lines, etc. These must be installed at the time of the continuity event.

3.6.1 Devolution of Operations/Transfer of Operations from Primary Worksite to Alternative Worksite

Operational control is transferred to an AWS through a process known as devolution. This involves the transfer of control (i.e., decision-making, direction, and control) from the primary worksite to the

AWS. Key personnel must arrive at the AWS and, when ready, assume control and initiate operations. Personnel should be prepared to relocate to the appropriate AWS to resume operations.

Equipment and supplies may need to be moved to the AWS. If possible, a cache of materials should be maintained at the AWS for immediate use. Emergency procurement of equipment and supplies may be required to replace items that are damaged, missing, or inaccessible. The PSAP manager will maintain a list of qualified vendors and manage emergency procurement activities.

An incident task list is a quick reminder of the steps you will need to complete during the AWS incident. The task list in Appendix D can be modified for your PSAP.

3.6.2 Vital Records and Databases

Vital records are those records that must be preserved, protected, and available for use by PSAP personnel at the AWS during or immediately following a continuity event. Examples include local hard drives, shared network drives, and/or external devices, an offsite data facility, or a cloud-based solution. A sample can be found in Appendix C.

3.7 Threat Readiness Levels

PSAP personnel should maintain a constant state of readiness to respond to disruptive events. General guidance for readiness levels, based upon threat conditions, is presented below.

Level 4: Normal Conditions

Level 4 Normal is maintained during periods of low risk. No specific threats have been identified and no immediate emergency events are anticipated.

Examples of Level 4 tasks include:

- Register and maintain subscriptions to electronic alerting sources (i.e., the National Oceanic and Atmospheric Administration [NOAA], CodeRed, etc.)
- Maintain NOAA weather emergency radio in PSAP
- Conduct ongoing risk assessments
- Review and maintain emergency response plans
- Train staff on emergency response procedures
- Prepare and maintain emergency supplies (e.g., first-aid kits, flashlights, face masks)
- Maintain fire-protection and security systems
- Conduct and assess lock-down, shelter-in-place, and evacuation drills
- Test AWS activation and devolution procedures
- Encourage personnel to conduct family preparedness measures

Level 3: Guarded/Increased Readiness

Level 3 Guarded indicates that conditions are present or favorable for a disruptive event or emergency to occur. This includes the threat of severe weather or a significant event that is occurring in the community, such as a hazardous materials spill.

Examples of Level 3 tasks include:

- Monitor official sources of warning for changing conditions
- Brief staff on developing situations
- Test internal communication plans
- Communicate condition status changes to partner organizations
- Check availability of emergency supplies and personal protective equipment (PPE)

Level 2: High Alert/Heightened Readiness

Level 2 High Alert indicates that conditions are present or highly conducive for an emergency event. A constant state of alert is mandated to monitor developing conditions until the threat subsides or escalates to an active emergency. Level 2 activation would be appropriate for an approaching storm.

Examples of Level 2 tasks include:

- Continue monitoring developing conditions through media, weather radio, and local government alerting staff
- During the workday, alert personnel to developing conditions
- Prepare personnel to shelter in place or evacuate facilities
- Prepare to implement facility lock-down procedures
- Place AWS on standby for activation

Level 1: Emergency Response

Moving to Level 1 status indicates that an emergency event is occurring that involves the PSAP's facilities. This may include an act of violence, fire-alarm activation, bomb threat, hazardous materials release, or other incident that requires immediate action to protect life and property and sustain operations.

Examples of Level 1 tasks include:

- Implement lock-down procedures
- Implement sheltering-in-place procedures
- Evacuate the facility
- Dismiss non-essential personnel and cancel activities
- Activate AWS and initiate workforce devolution procedures

4. INCIDENT MANAGEMENT

4.1 General

Most continuity events are of short duration with limited impact on the organization. During those incidents, the PSAP will continue to operate using the normal organizational structure. Larger or significant incidents will require activation of the COOP Plan and the implementation of an incident management team (IMT). The PSAP will continue to operate using the normal organizational structure until an alternate command and control structure is implemented.

4.2 COOP Plan Activation

The PSAP manager/director/other or their designee is authorized to activate the COOP Plan.

4.3 Incident Management Team

The IMT concept is used to coordinate the response to an emergency event that disrupts normal operations. Members of the IMT will be comprised of PSAP staff based on their leadership roles and technical expertise.

The PSAP will utilize its normal organizational structure to manage the response to short-term continuity events. Complex or long-term incidents will require the IMT to use the National Incident Management System (NIMS) methodology. IMT members should complete NIMS training and participate in exercises to test their ability to operate using the NIMS methodology.

4.4 Incident Action Plan

The Incident Action Plan (IAP) is a tool to aid the organization in managing the response to a disruptive incident. The IAP is used to capture information that is relevant to the incident, including incident type, location(s) impacted by the incident, situation summary, operational period, incident objectives, IMT members and roles, external resources, and management approval. The IAP was formatted for use by individuals who do not frequently operate under the NIMS methodology. Digital and printed versions of the IAP form (blank) should be maintained and accessible during an emergency. Refer to Appendix E for instructions on completing the IAP.

4.5 Crisis Communications

The PSAP manager/director is responsible for coordinating information during an emergency that disrupts 911 service. PSAP internal communications procedures utilize a combination of voice, text, and email to communicate with staff. The crisis communications procedures address the following:

- Staff notification and communication procedures
- Coordination with other agency departments
- Coordination with partner agencies
- Coordination with PSAP manager and senior officials
- Coordination with contractors and vendors
- Public information and media relations

Person-to-person voice communication is the most effective method to assure that messages and instructions are properly conveyed. Personal contact between supervisors and subordinates is the preferred method of coordinating resources. The process simply requires that each supervisor personally contact his or her immediate subordinates. Supervisors will document the time that each employee was contacted and their status or availability to report for a work assignment.

Text messaging and email are alternative methods to contact staff members. Both can be effective in reaching multiple recipients simultaneously. However, it is difficult to track replies to text and email messages and verify that the intended recipient(s) received and read messages.

4.6 Personnel Safety and Accountability

A continuity event can affect the health and safety of the PSAP staff. When a disruptive event occurs, personnel may be in the facility, at home, or traveling outside of the area. The PSAP supervisor must account for all employees during and after the occurrence of a continuity event. The emergency notification process will involve documenting the employee's location, the status of their health and safety, and their availability to report for work.

The PSAP should use a dedicated non-published telephone number for personnel accountability. Staff members will use the number to report their status and receive instructions and duty assignments. Personnel assigned to monitor the phone will maintain a log of staff contacts and document the status of each employee. An emergency contact list for personnel will be maintained separately from this plan in digital and print formats. The contact list must be updated monthly.

If your PSAP uses an emergency notification system, ensure you have a hard copy of contact information in the event systems are down.

Staff working in the field should identify facilities in which they can take shelter during an emergency (i.e., tornado warning). The staff member should report their status and location to a supervisor upon taking shelter.

4.7 Government Emergency Telecommunications Services

Depending on the incident and impact, first responders may require an alternate path to place wireless and landline calls. The Government Emergency Telecommunications Service (GETS) provides first responders priority access and prioritized processing in the local and long-distance segments of the landline networks, greatly increasing the probability of call completion.[9]

Two other related segments provide priority on the wireless network (Wireless Priority Services [WPS]) and other vital voice and data circuits or other telecommunications services (Telecommunications Service Priority [TSP]). Users can obtain more information or sign up for services at the DHS Priority Telecommunications Service Center.

5. RECOVERY AND RECONSTITUTION

5.1 General

Post-incident recovery involves evaluating the status of PSAP resources following a disruptive incident and reorganizing to secure resources to maintain operational capacity. Reconstitution is the process of resuming normal operations at the primary work site, AWS, or temporary/permanent replacement facility.

Recovery and reconstitution activities will be implemented to restore routine operations of the PSAP. The PSAP must be prepared to support recovery on two levels. The first level, continuity of operations, involves the human and physical resources that are necessary to provide services to served agencies and the public. The second level, disaster recovery, involves the recovery of IT

[9] https://www.cisa.gov/government-emergency-telecommunications-service-gets

equipment, systems, applications, and networks. The recovery process involves establishing and prioritizing short-term and long-term objectives.

Examples of short-term recovery objectives include:

- Provide for the needs and well-being of PSAP staff
- Assess damages
- Communicate with stakeholders
- Activate vendor support agreements
- Relocate to AWS
- Restore essential systems and services
- Recover data

Examples of long-term recovery objectives include:

- Replace equipment
- Hire temporary or permanent staff
- Restore primary worksite
- Relocate to permanent worksite

6. COOP TRAINING AND EXERCISES

6.1 General

Exercises are used to test and validate planning assumptions, tasks, and procedures. The PSAP should test and revise its COOP Plan annually and ensure staff are trained and tested in its use regularly.

6.2 Training

PSAP staff and members of partner organizations must be trained in the use of the COOP Plan. Training is intended to strengthen capabilities that are needed to respond to and recover from a continuity event. Topics for training include:

- Threat monitoring, alerting, and warnings
- Emergency response procedures
- Crisis communications procedures and processes
- Establishing alternate PSAP and devolution procedures
- Reconstitution operations procedures

6.3 Exercises

The PSAP should conduct preparedness exercises to test and validate procedures and planning assumptions, test new equipment, and refine personnel capabilities. The PSAP will utilize exercises to assess continuity capabilities. Exercises should be conducted in coordination with partner agencies and the local office of emergency management.

6.4 After-Action Reporting

Training and real-world events represent opportunities for organizations to implement plans and assess response capabilities. Drills, exercises, and responses to actual emergency events should be documented using an after-action report (AAR)/improvement plan format.

An AAR template can be found in Appendix F.

7. PLAN ADMINISTRATION AND MAINTENANCE

7.1 Plan Distribution and Access

A COOP Plan contains sensitive security information that should be restricted from public access. The distribution plan must be approved by PSAP leadership. Distribution of the COOP Plan is limited to essential personnel and authorized representatives of partner agencies and contractors. Copies of the COOP Plan should be maintained both at the facility and offsite in print and digital format.

7.2 Plan Maintenance

PSAP leadership is responsible for assuring that the COOP Plan is maintained and tested annually. The review process should include an assessment of changes in hazards, threats, personnel assignments, facilities, hardware, and other resources.

7.3 Records and Reports

Records related to the activation of the COOP Plan must be maintained in compliance with state law and record-retention policies. Documentation of disaster-related expenses will be needed to support cost recovery requests. Examples of preparedness and incident-related reports include:

- COOP Plan
- Exercise and actual event AAR/improvement plan
- Personnel and payroll records
- Purchase orders, receipts, and contracts
- Reports of injuries and workers' compensation documents
- Other administrative data and reports related to incidents

APPENDIX A – ORDERS OF SUCCESSION AND DELEGATIONS OF AUTHORITY

Use the table below to identify positions within the PSAP that are essential to maintain operations. In addition to the incumbent, two alternate individuals should be identified to ensure enough staffing in the absence of the incumbent. List key MEFs that are assigned to the position and any legal authorities to be delegated to the person temporarily filling the position (e.g., hiring, budget, purchasing, etc.). (Note: All positions should be listed by title and not by names of individuals serving in the position.)

The following are examples for use. Fill in the information as appropriate for your PSAP.

Staff Positions Example

PSAP Director
Alternate 1: PSAP Manager
Alternate 2: GIS Administrator
Essential Tasks to Perform: Responsible for the overall operation of the PSAP including supervision of department staff, planning, budgeting, procurement, accounts payable, contract management, vendor management, public information, network design, and all other areas related to the operation of the 911 network. In addition, the PSAP Director is the primary point of contact with local elected officials, news media, public, vendors, and other stakeholders.
Authority to be Delegated: Act as a decisionmaker in absence of the PSAP Director.

PSAP Manager
Alternate 1: Supervisor 1
Alternate 2: Supervisor 2
Essential Tasks to Perform: Responsible for overseeing the PSAP's ongoing operations, which include performance staff supervision, working with the sheriff and other elected officials, and region-wide public education/awareness. Program and PSAP monitoring and compliance, and other tasks related to operations of the 911 program. Is authorized to act and make routine decisions in absence of the Director. Manage backup/training PSAP and ensure complete operability. Coordinate and conduct training for telecommunicators.

PSAP Manager
Authority to be Delegated: Manage backup/training PSAP and ensure complete operability. Coordinate and conduct training for telecommunicators. Program and PSAP monitoring and compliance, and other tasks related to operations of the 911 program.

GIS Administrator
Alternate 1:
Alternate 2:
Essential Tasks to Perform: Manages the technical components of the program's GIS, including software, hardware, and database administrative activities. Troubleshooting GIS problems. Coordinate map production for first responders during disasters.
Authority to be Delegated: Manages the technical components of the program's GIS, including software, hardware, and database administrative activities. Troubleshooting GIS problems. Coordinate map production for first responders during disasters.

Supervisor 1
Alternate 1:
Alternate 2:
Essential Tasks to Perform:
Authority to be Delegated:

Supervisor 2
Alternate 1:
Essential Tasks to Perform:
Authority to be Delegated:

Administrative Coordinator
Alternate 1:
Alternate 2:
Essential Tasks to Perform: Code program accounts payables. Verify billings for accuracy.
Authority to be Delegated: Code program accounts payables. Verify billings for accuracy.

Information Technology Director
Alternate 1: Contracted Services
Alternate 2: N/A
Essential Tasks to Perform: For non-911-specific hardware and software. Leads in planning, design, documentation, and implementation of various systems to include desktop PCs, servers, network equipment, software applications, firewalls, and security/camera systems.
Authority to be Delegated: For non-911-specific hardware and software. Leads in planning, design, documentation, and implementation of various systems to include desktop PCs, servers, network equipment, software applications, firewalls, and security/camera systems.

APPENDIX B – MISSION ESSENTIAL SYSTEMS AND SOFTWARE APPLICATIONS

This section should detail the MEFs and technologies used within the PSAP at both the primary and secondary sites.

Network diagrams of the default routing schemas can be included in this section. A list of equipment, software version, and vendor contact information is also appropriate for this section.

Mission Essential Hardware--Site Inventory

Essential Hardware					
Equipment Description	**Manufacturer/ Vendor**	**Model Number**	**Serial Number**	**Owned/ Leased**	**Vendor/Support Contact**

Mission Essential Software Applications--Site Inventory

Application Inventory				
Manufacturer/ Vendor	**Application Name**	**Version #**	**Application Interfaces/Dependencies***	**Service Level Agreement**

*Data requirements, interfaces, processing relationships, etc.

Identify application dependencies such as what related processes must be available for each application to function properly?

Vendor Contracted Services

Vendor Contacts				
Application/Hardware	**Vendor**	**Point(s) of Contact**	**Phone Number**	**Account Number**

Vendor Managed – Customer Handling Equipment (CHE) Inventory

Host Site CHE Cabinet Hardware inventory	AWS CHE Cabinet Hardware Inventory
Equipment Description	**Equipment Description**

It is important to capture the circuit identification (ID) numbers of each carrier that provides telecommunications services for the PSAP including 911 trunks and administrative lines. A table is provided below to document circuit IDs and carrier contact information for trouble reporting.

Telecommunication Carrier Circuit IDs

Vendor Contacts				
Carrier	**Circuit ID**	**Point(s) of Contact**	**Phone Number**	**Account Number**

APPENDIX C – ALTERNATIVE WORKSITE (AWS)

AWS Activation

The PSAP manager/director or their designated alternate(s) is authorized to activate the AWS. This includes notifying the official in charge of the site and arranging for the transport or delivery of equipment and supplies. This is also the section for vital record information.

Contact the following representatives of the AWS to request site activation.

AWS Contact Information

Primary Contact	Alternate Contact
Facility Name:	Facility Name:
Facility Address:	Facility Address:
Contact Name:	Contact Name:
Telephone:	Telephone:
Telephone:	Telephone:
Email:	Email:
Other:	Other:

[INSERT MAP TO AWS]

Equipment and Supplies to Transport to the AWS

Equipment and Supplies to Transport to AWS	

Vital Records and Data

Vital Records and Data			
Record Type	**Data Type**	**Offsite Backup**	**Backup Frequency**

APPENDIX D – INCIDENT TASK LIST

The information presented in the following tables is an example of the use and development of an Incident Task List. These tasks should be modified for your PSAP. The list below is an example provided by a Nebraska county.

Incident Task List	
Stage I: Short-term Activation (Day 1 at AWS) **Goal: Attain operational status within [12] hours**	
Task	Completed
Notify department personnel that the COOP Plan has been activated and devolution/relocation procedures are being implemented (include IT or appropriate departments that manage network and equipment at AWS)	
Contact the AWS representative to confirm that the site is available to support the relocation of department personnel and coordinate site access	
Determine which members of the Continuity Team are to report immediately and who is on call	
Contact Continuity Team and advise them of their status (report or on-call)	
Convene at the designated AWS per Continuity Management Team (CMT) instructions	
At AWS—coordinate with the CMT for specific seat assignments	
Verify availability of necessary office supplies (i.e., paper, envelopes, pens, pencils, forms, paperclips, stapler, staples, etc.)	
Verify access to items on the Equipment list using recovery time objective priority order	
Verify access to computer systems and software on the Computer Programs list using recovery time objective priority order	
Verify access to items on the Vital Records list using recovery time objective priority order. Coordinate retrieval of offsite, as required	
Review Communications Contact list and make necessary contacts, as required, to alert them of the situation and/or solicit support. (Notify the EOC or EMA that department operations have been initiated at the AWS. Notify officials, media contacts, vendors, etc.)	
Advise CMT of the Office's recovery status	
Brief department staff regarding site operation procedures	

Incident Task List	
Stage I: Short-term Activation (Day 1 at AWS) **Goal: Attain operational status within [12] hours**	
Task	Completed
Begin performing functions/processes on the Function/Process list using recovery time objective priority order	
Determine work schedules and staffing needs for the remainder of the week	
Contact employees currently on call and advise them of their status and work schedule	
Provide scheduled situation updates to the appropriate point of contact at the EOC	
Provide situation updates to staff working at the AWS at regular intervals	
Track hours, overtime and receipts for items purchased	

Incident Task List	
Stage II: Long-term Activation (Up to 30 days at AWS)	
Task	Completed
Continue to monitor the Function/Process list to add functions, as staff and time allows	
Advise CMT of the Office's resumption of process and staffing status	
Continue to review Communications Contact list and make necessary calls, as required to advise or coordinate	
Determine and set up workspace for additional staffing using Minimum Operating Requirements as a guide	
Order and replenish equipment and supplies, as required and coordinate with CMT	
Track hours, overtime, and receipts for items purchased	
Assist with clean up and/or salvage operations (refer to Vital Records and Equipment tables for target salvage items	
Determine inventory of usable equipment, documents, and materials	
Assist with determining losses for insurance carriers, if required. Coordinate with Management Team	
Provide briefing to entire office staff	

Incident Task List	
Stage II: Long-term Activation (Up to 30 days at AWS)	
Task	Completed
Prepare and present briefing for customers, vendors, and suppliers, as required	
Assist with developing long-term recover strategy/reconstitution activities	
Monitor workforce stress caused by the relocation	

Incident Task List	
Stage III: Extended Relocation:	
Task	Completed
Assess the need to relocate department operations to another location (i.e., leased space or other governmental jurisdiction)	
Negotiate and execute a commercial lease or an interlocal agreement for the extended use space not owned by the County	

APPENDIX E – INCIDENT ACTION PLAN AND CONTINUITY TASKS

The IAP document is intended for use during an emergency incident. The IAP contains information regarding the nature of the incident, response strategy for managing the incident, staff assignments, and objectives to achieve during a prescribed operational period.

Blank copies of the IAP document should be readily available to staff in digital and print formats. This section presents the IAP form and an explanation of its preparation and use.

CONTINUITY OF INCIDENT ACTION PLAN

Incident Type	Prepared By	Date	Time
Incident Location (s)			
Operation Period	Date: From_____ To_____	Time: From_____ To_____	
Situation Summary and Priorities			
Hazards and Safety Measures			

Incident Objectives		
Objectives	Strategy and Resources Required	Assigned To

Incident Management Team (IMT) Members and Assignments		
Name	Position/IMT Role	Contact Information
		Phone: Email:
		Phone: Email:

		Phone: Email:
		Phone: Email:
		Phone: Email:
External Resources		
Contractor/Vendor Name	Services Provided	Contact
		Phone: Email:
		Phone: Email:
		Phone: Email:
		Phone: Email:
Attachments		
Approved By:	Date:	Time:

Continuity IAP Instructions

Purpose

The IAP is a tool to aid the organization in managing the response to a disruptive incident. The IAP is used to capture incident type, location or locations impacted by the incident, situation summary, operational period, incident objectives, IMT members and roles, external resources, and approval.

Preparation

The IAP is typically completed by the individual assigned to lead the organization's response and recovery efforts. The IAP is reviewed and approved by a senior representative such as a director, sheriff, chief, or city manager. Information entered on the form should be clear and concise.

Distribution

The IAP should be distributed to all individuals involved in leading incident response and recovery efforts. The priorities and objectives should be presented during briefings to the IMT. Copies of each IAP must be retained for use in the incident documentation and post-incident review(s).

Incident Priorities

The initial stages of a disruptive incident may be chaotic and confusing. It may be difficult to identify the extent of disruptions and damages due to a lack of situational awareness. The IAP is intended to provide individuals responsible for managing the incident response with coordinating information needed to establish actionable priorities and objectives.

Initial priorities will begin with broad and generic language due to the lack of specific information. Examples of initial priorities may include:

- Establish the IMT
- Account for the health and safety status of all personnel
- Determine the status of partner agencies
- Identify the extent of disruption to normal operations
- Determine the level of damage to facilities
- Restore essential services
- Recall off-duty personnel to support response efforts

Priorities will progress to include more specific actions such as:

- Establish defined operational periods
- Restore electrical service
- Request emergency assistance from contractors and vendors
- Conduct damage assessment of the primary facility

Incident Objectives

Incident objectives provide direction and help focus the IMT's actions throughout the response and recovery phases of the incident. Incident objectives are more immediate than priorities and represent a target to be attained during the operational period. Objectives provide a means to measure progress achieved during an operational period. The characteristics of effective incident objectives should reflect the ***SMART*** concept. Incident objects should be:

Specific. Contain specific direction regarding the five W's – who, what, when, where, and why. The objective should specify a timeframe in which it should be accomplished.

Measurable. Include metrics that describe observable actions and outcomes.

Achievable. Be within the control, influence, and realistic application of available resources.

Relevant. Be related to the mission of the organization and related to goals and strategic intent.

Time-bound. Include a reasonable timeframe for completion.

The following table is a guide that describes the information that should be entered into each section of the IAP.

Item No.	Section Title	Instructions
1.	Incident Type	Enter the type of incident that has occurred (i.e., flood, fire, power outage, etc.).
2.	Prepared By	Enter the name of the person completing the IAP.
3.	Date	Enter the date the IAP was prepared.
4.	Time	Enter the time the IAP was prepared.
5.	Incident Location(s)	Enter the location (or locations) that are affected by the incident, including addresses.
6.	Operational Period	Enter the time that the IAP covers. The typical operational period is 8–12 hours.
7.	Situation Summary and Priorities	Enter a summary of the current conditions that exist at the beginning of the operational period. The summary should include the priorities for the operational period.
8.	Hazards and Safety Measures	Enter the hazards that currently exist, and precautions being taken to protect personnel.
9.	Incident Objectives A. Objectives B. Strategy and Resources Required C. Assigned To	A. Enter each objective that has been defined for the operational period. Objectives should clearly reflect the SMART concept. B. Describe the strategy and resources necessary to achieve the objective. C. Enter the name of the individual responsible for leading the efforts to attain the objective.
10.	Incident Management Team (IMT) Members and Assignments Name Position/IMT Role Contact Information	Enter the name, position/role, and contact information for members of the IMT.
11.	External Resources Contractor/Vendor Name Services Provided Contact	Enter the name of contractor or vendor organizations supporting the operational period. Enter the services being provided and contact information for vendor representatives.
12.	Attachments	List any additional documents that are attached to the IAP.
13.	Approved By	Enter the name of the person reviewing and approving the IAP.
14.	Date and Time	Enter the date and time that the IAP was approved.

APPENDIX F – AFTER-ACTION REPORT TEMPLATE

The information below is an AAR template that can be used to assess and follow-up after an incident.

After-Action Report Template

Introduction
Include a brief synopsis of the incident *Include a sequence of events (if available)*
After Action Report (AAR) Overview
This report is a compilation of information from the different departments and staff who participated in the response to *[list incident/exercise/event here]*. The information was gathered by *[list departments here and various sources of information for the report].* The recommendations in this AAR should be viewed with considerable attention to providing safe care to residents. Each department should review the recommendations and determine the most appropriate action and time needed for implementation. The issues outlined in this AAR will be addressed in the Improvement Plan and will list corrective actions to complete. The Improvement Plan will serve as a summary of the AAR and as a guide for corrective action over the course of the following year's training program for staff.
Incident Overview:
[Insert incident/exercise/event location here]
Duration:
[Insert incident/exercise /event time]

Focus *(Check appropriate area(s)**:***	***Activity/Scenario*** *(Check appropriate area(s):*
☐ Prevention	☐ Fire
☐ Response	☐ Severe Weather
☐ Recovery	☐ Hazardous Material Release
☐ Other	☐ Bomb Threat
	☐ Medical Emergency
	☐ Power Outage
	☐ Evacuation
	☐ Lockdown
	☐ Special Event
	☐ Exercise/Drill
	☐ Other

Location:
[Insert incident/exercise/event location here]
Participating Organizations:
[Insert organizations here]
Strengths:
[List strengths here]
Areas of Improvement:
[List areas of improvement here]
Recommendations
[List recommendations here]
Conclusion and Next Steps
[Insert conclusion here]

APPENDIX G – AUTHORITIES AND REFERENCES

Authorities

A. The Nebraska Emergency Management Act, Neb. Rev. Stat. §§ 81-829.36 to 81-829.75

B. 911 Service System Act, Act, Neb. Rev. Stat. §§ 86-1001 to 86-1029.03

C. Emergency Telephone Communications Systems Act, Neb. Rev. Stat. §§ 86-420 to 86-441.01

D. Enhanced Wireless 911 Services Act, Neb. Rev. Stat. §§ 86-442 to 86-470

E. [PSAP NAME] Interlocal Agreement for E911 Public Safety Answering Point Services

References

1. Federal Communications Commission, *Emergency Planning: Public Safety Answering Points*, August 23, 2016. https://www.fcc.gov/research-reports/guides/emergency-planning-public-safety-answering-points

2. NENA-INF-017.3-2018, *NENA Communications Center/PSAP Disaster and Contingency Plans Model Recommendation*, September 28, 2018. https://www.nena.org/resource/resmgr/standards/nena-inf-017.3-2018_disaster.pdf

3. NENA 75-001, *NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)*, Version 1, February 6, 2010. https://www.nena.org/page/NG911_Security

4. NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems*, 2019. https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1221

5. NFPA 1600, *Standard on Continuity, Emergency, and Crisis Management*, 2019. https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1600

6. FEMA, *Continuity of Operations Plan Template and Instructions for Federal Departments and Agencies,* July 2011. https://www.fema.gov/pdf/about/org/ncp/coop/continuity_plan_federal_d_a.pdf

7. FEMA Comprehensive Preparedness Guide (CPG) 101, *Developing and Maintaining Emergency Operations Plans,* Version 2, November 2010. https://www.fema.gov/emergency-managers/national-preparedness/plan#cpg

8. NENA-INF-019.2-2016, *NENA Resource, Hazard and Vulnerability Analysis Information Document*. Hazard & Vulnerability Analysis - National Emergency Number Association (nena.org)

9. APCO/NENA ANS 1.102.3-2020, *Emergency Communications Center (ECC) Service Capability Rating Scale*. https://www.apcointl.org/download/ecc-service-capability-criteria-rating-scale/?wpdmdl=6344

10. Homeland Security Presidential Directive-7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection (2003)*. https://www.cisa.gov/homeland-security-presidential-directive-7

11. U.S. Department of Health and Human Services (HHS), *Pandemic Influenza Plan 2017 Update*. https://www.cdc.gov/flu/pandemic-resources/pdf/pan-flu-report-2017v2.pdf

12. National 911 Program, Coronavirus/COVID 19 Resources. https://www.911.gov/project_coronavirus_covid-19_resources.html

13. CISA*, Guidelines for 911 Centers: Pandemic Planning*, https://www.cisa.gov/sites/default/files/publications/CISA%20Pandemic_EmergencyCommsCenters_Planning_05.13.20%20%28508c%29.pdf

14. National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, April 2018. https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

15. Federal Emergency Management Agency (FEMA), *Incident Action Planning Guide*, July 2005. https://www.fema.gov/sites/default/files/2020-07/Incident_Action_Planning_Guide_Revision1_august2015.pdf

16. FEMA: Federal Continuity Directive 1 *Federal Executive Branch National Continuity Program and Requirements*, January 17, 2017. https://www.fema.gov/sites/default/files/2020-07/January2017FCD1.pdf

17. FEMA: Federal Continuity Directive 2 *Federal Executive Branch Mission Essential Functions and Candidate Mission Essential Functions Identification and Submission Process*, June 13, 2017. https://www.fema.gov/sites/default/files/2020-07/fema_federal-continuity-directive-2_061317.pdf

APPENDIX H – ACRONYMS LIST

AAR	After-action Report
APCO	Association of Public-Safety Communications Officials International
AWS	Alternate worksite
CAD	Computer-aided Dispatch
CHE	Call-handling Equipment
CISA	Critical Infrastructure and Cybersecurity Agency
CMT	Continuity Management Team
COOP	Continuity of Operations
DHS	Department of Homeland Security
ECC	Emergency Communications Center
EMA	Emergency Management Agency
EMS	Emergency Medical Services
EOC	Emergency Operations Center
FEMA	Federal Emergency Management Agency
GETS	Government Emergency Telecommunications Service
GIS	Geographic Information System
IAP	Incident Action Plan
ICS	Incident Command System
ID	Identification
IMT	Incident Management Team
IP	Internet Protocol
IT	Information Technology
MEF	Mission Essential Function
NENA	National Emergency Number Association
NFPA	National Fire Protection Association
NIMS	National Incident Management System
NOAA	National Oceanic and Atmospheric Administration
PPE	Personal Protective Equipment
PSAP	Public Safety Answering Point
PST	Public Safety Telecommunicator
RMS	Records Management System
RPO	Recovery Point Objectives
RTO	Recovery Time Objectives
SLA	Service Level Agreement
SPOF	Single Point of Failure
TSP	Telecommunications Service Priority
WPS	Wireless Priority Services

APPENDIX I – CONTINUITY GLOSSARY

Alert. Notification that a potential emergency or disaster situation is imminent, exists or has occurred; usually includes a directive for personnel to stand by for possible activation.

Alternate Worksite (AWS). 1) An alternate operating location to be used by business functions when the primary facilities are inaccessible. 2) Another location, computer center, or work area designated for recovery. 3) A location, other than the main facility, that can be used to conduct business functions. 4) A location, other than the normal facility, used to process data and/or conduct critical business functions in the event of a disaster.

Application Recovery. The component of disaster recovery that deals specifically with the restoration of business system software and data after the processing platform has been restored or replaced.

Assembly Area. The designated area at which employees, visitors, and others are to assemble if evacuated from a building or worksite.

Call Tree. A document that graphically depicts the calling responsibilities and the calling order used to contact management, employees, customers, vendors, and other key contacts in the event of an emergency, disaster, or severe outage situation.

Cold Site. An alternate facility that already has in place the environmental infrastructure required to recover critical business functions or information systems, but does not have any pre-installed computer hardware, telecommunications equipment, communication lines, etc. These systems must be provisioned at the time of disaster.

Continuity Event. Any event that causes an agency to relocate its operations to an alternate or other continuity site to assure continuance of its essential functions.

Continuity of Operations (COOP) Plan. A COOP plan provides guidance on the system restoration for emergencies, disasters, mobilization, and for maintaining a state of readiness to provide the necessary level of information-processing support commensurate with the mission requirements/priorities identified by the respective functional proponent. The federal government and its supporting agencies traditionally use this term to describe activities otherwise known as Disaster Recovery, Business Continuity, Business Resumption, or Contingency Planning.

Critical Infrastructure. Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any federal, state, regional, territorial, or local jurisdiction.

Cybersecurity. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks; wireline, wireless, and satellite communications networks; PSAPs; 911 communications systems; and control systems.

Damage Assessment. The process of assessing damage to computer hardware, vital records, office facilities, etc., and determining what can be salvaged or restored and what must be replaced following a disaster.

Delegation of Authority. Identification, by position, of the authorities for making policy determinations and decisions. Generally, pre-determined Delegations of Authority will take effect when normal channels of direction have been disrupted and will lapse once these channels have been restored.

Dependency. The reliance or interaction of one activity or process upon another.

Devolution of Operations. The capability to transfer statutory authority and responsibility for essential functions from an agency's primary operating staff and facilities to other agency employees and facilities, and to sustain that operational capability for an extended period.

Disaster. Any event that can cause a significant disruption to emergency call capability, as defined by NENA.

Disaster Recovery. A specific set of procedures designed to reduce the damaging consequences of unexpected events resulting in the loss of 911 call handling or dispatching capabilities. The collection of resources and activities to re-establish information technology (IT) services (including components such as infrastructure, telecommunications, systems, applications, and data) at an alternate site following a disruption of IT services. Disaster recovery includes subsequent resumption and restoration of those operations at a more permanent site.

Emergency. An unexpected or impending situation that may cause injury, loss of life, or destruction of property, or cause the interference, loss, or disruption of an organization's normal business operations to such an extent that it poses a threat.

Emergency Operations Center (EOC). The physical and/or virtual location from which strategic decisions are made and all activities of an incident are directed, coordinated, and monitored.

Evacuation. The movement of employees, visitors, and contractors from a site and/or building to a safe place (assembly area), in a controlled and monitored manner at the time of an event.

Exercise. A tool used to train for, assess, practice, and improve performance in a risk-free environment. Exercises can be used for testing and validating policies, plans, procedures, training in the use of new equipment, and interagency agreements; clarifying and training personnel in roles and responsibilities; improving interagency coordination and communications; improving individual performance; identifying gaps in resources; and identifying opportunities for improvement.

Hazard. Something that is potentially dangerous or harmful, often the root cause of an unwanted outcome.

Hot Site. An alternate facility that already has in place the computer, telecommunications, and environmental infrastructure required to recover critical business functions or information systems.

Incident Command System (ICS). The combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, with responsibility for the

command, control, and coordination of assigned resources to effectively direct and control the response and recovery to an incident.

Mission-Critical Activities. The critical operational and/or business support activities (either provided internally or outsourced) required by the organization to achieve its objective(s) (i.e., services and/or products).

Mission-Critical Application. Computer applications that support activities or processes that cannot be interrupted.

Mission Essential Function. A function or task that is necessary for personnel to perform to maintain mission-critical services.

Mitigation. Ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident. The capabilities necessary to reduce loss of life and property by lessening the impact of disasters.

Mobile Recovery. A mobilized resource purchased or contracted for the purpose of business recovery. The mobile recovery center might include computers, workstations, telephony, electrical power, etc.

Network Outage. An interruption of voice, data, or Internet Protocol (IP) network communications.

Outage. The interruption of automated processing systems, infrastructure, support services, or essential business operations, which may result in the organization's inability to provide services for some period.

Orders of Succession. A sequential listing of organization positions (rather than specific names of individuals) that define what position is authorized to assume a specific role under emergency circumstances.

Preparedness. Activities necessary to build, sustain, and improve readiness capabilities to prevent, protect against, respond to, and recover from natural or manmade incidents. A continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action to ensure effective coordination during incident response.

Prevention. Actions initiated, and measures put in place for the continual assessment and readiness of necessary actions to reduce the risk of threats and vulnerabilities, to intervene and stop an occurrence, or to mitigate effects.

Primary Operating Facility. The facility where an organization conducts operations on a day-to-day basis.

Protection. Actions or measures taken to cover or shield from exposure, injury, or destruction. In the context of 911 infrastructure, protection includes actions to deter the threat, mitigate the vulnerabilities, or minimize the consequences associated with a terrorist attack or other incidents.

Recovery. The development, coordination, and execution of service- and site-restoration plans for affected communities, and the reconstitution of government operations and services.

Recovery Point Objectives (RPO). The predefined time in which data is restored and/or systems recovered after a disruption or outage.

Recovery Time Objectives (RTO). The target time within which systems, applications, or functions must be recovered after an outage. RTO includes the time required for assessment, execution, and verification. RTO may be enumerated in operational time (e.g., one shift day) or elapsed time (e.g., 24 elapsed hours).

Redundancy. The state of having duplicate capabilities such as systems, equipment, and other resources.

Resilience. The ability of an organization to absorb the impact of a business interruption and continue to provide a minimum acceptable level of service.

Response. The reaction to an incident or emergency to assess the damage or impact and to ascertain the level of containment and control activity required. In addition to addressing matters of life safety and evacuation, Response also addresses the policies, procedures, and actions to be followed in the event of an emergency.

Risk. Potential for exposure to loss that can be determined by using either qualitative or quantitative measurements.

Scenario. Provides the storyline that drives an exercise to test objectives. The scenario selected for an exercise should be informed by the actual threats and hazards faced by the exercise stakeholders. The exercise scenario should realistically stress the delivery of core capabilities, providing a mechanism for testing objectives and assessing core capability levels and gaps.

Service Level Agreement (SLA). A formal agreement between a service provider (whether internal or external) and their client (whether internal or external), which covers the nature, quality, availability, scope, and response of the service provider. The SLA should cover day-to-day situations and disaster situations, as the need for the service may vary in a disaster.

Single Point of Failure (SPOF). A unique pathway or source of a service, activity, and/or process. Typically, there is no alternative, and a loss of that element could lead to a failure of a critical system.

Telephone Tree. A list of staff, their phone numbers, and their role in the ICS (if applicable) The first person on the list (usually the principal or incident commander) calls his or her pre-assigned staff members to relay what is and is not known and what steps should be taken. These staff members continue passing along the principal’s message to their pre-assigned contacts until everyone has been notified.

Telework. Allows employees to conduct some or all of their work at an AWS away from the employee's typically used office, because that may not be viable during an emergency.

Threat. Natural, technological, or human-caused occurrence, individual entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Vulnerability. A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

Warm Site. A designated AWS that is equipped with some hardware, communications interfaces, electrical, and environmental conditioning, but which is only capable of providing backup after additional provisioning, software installation, or customization is performed.

Warning. The alerting of emergency response personnel and the public to the threat of extraordinary danger and the related effects that specific hazards may cause. A warning issued by the National Weather Service (e.g., severe storm warning, tornado warning, or tropical storm warning) for a defined area indicates that the severe weather is imminent in that area.

Watch. Indication by the National Weather Service that in a defined area conditions are favorable for the specified type of severe weather, such as flash floods, severe thunderstorms, tornadoes, and tropical storms.

Workspace. The physical building area where work is normally performed.

APPENDIX J – PANDEMIC DISEASE PREPAREDNESS AND RESPONSE

The National 911 Program has provided the PSAP community with multiple resources for preparing for and managing pandemic response. There is a document on the programs website (911.gov) titled *COVID-19 Pandemic Continuity of Operations Response Plan* for use in developing a unique plan that meets specific PSAP needs.