NENA Communications Center/PSAP Disaster and Contingency Plans Model Recommendation

NOTE: This DRAFT document is not intended for distribution beyond the groups developing or reviewing the document. The document is also not intended to be used or referenced for development or procurement purposes until final publication. All draft material is subject to change and it is possible that the document itself may never be approved for publication.

NENA Communications Center/PSAP Disaster and Contingency Plans Model Recommendation

NENA-INF-017.3-201Y
DSC Approval: MM/DD/YYYY
PRC Approval: MM/DD/YYYY
NENA Executive Board Approval: MM/DD/YYYY
Next Scheduled Review Date: MM/DD/YYYY (See ADM-002 Section 7.3.1 for details. The review date will be recommended by the Authoring Committee and once approved the date will be identified on the cover page of the document. Minimum 1 yr / Maximum 3-5 yrs)

Prepared by:
National Emergency Number Association (NENA) PSAP Operations Committee, Contingency Planning Subcommittee, Contingency Planning Document Review Work Group

Published by NENA
Printed in USA
This Information Document (INF) is published by the National Emergency Number Association (NENA) as an information source for 9-1-1 System Service Providers, network interface vendors, system vendors, telecommunication service providers, and 9-1-1 Authorities. It is not intended to provide complete design or operation specifications or parameters or to assure the quality of performance for systems that process such equipment or services.

NENA reserves the right to revise this Information Document for any reason including, but not limited to:

- Conformity with criteria or standards promulgated by various agencies,
- Utilization of advances in the state of the technical arts,
- Reflecting changes in the design of equipment, network interfaces, or services described herein.

This document is an information source for the voluntary use of communication centers. It is not intended to be a complete operational directive.

It is possible that certain advances in technology or changes in governmental regulations will precede these revisions. All NENA documents are subject to change as technology or other influencing factors change. Therefore, this NENA document should not be the only source of information used. NENA recommends that readers contact their 9-1-1 System Service Provider (9-1-1 SSP) representative to ensure compatibility with the 9-1-1 network, and their legal counsel to ensure compliance with current regulations.

Patents may cover the specifications, techniques, or network interface/system characteristics disclosed herein. No license expressed or implied is hereby granted. This document shall not be construed as a suggestion to any manufacturer to modify or change any of its products, nor does this document represent any commitment by NENA or any affiliate thereof to purchase any product whether or not it provides the described characteristics.

By using this document, the user agrees that NENA will have no liability for any consequential, incidental, special, or punitive damages arising from use of the document.

NENA’s Committees have developed this document. Recommendations for change to this document may be submitted to:

National Emergency Number Association
1700 Diagonal Rd, Suite 500
Alexandria, VA 22314
202.466.4911
or commleadership@nena.org

© Copyright YYYY National Emergency Number Association, Inc.
79 **Intellectual Property Rights (IPR) Policy**

80 NOTE – The user’s attention is called to the possibility that compliance with this document may require
81 use of an invention covered by patent rights. By publication of this document, NENA takes no position with
82 respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder
83 has filed a statement of willingness to grant a license under these rights on reasonable and
84 nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be
85 obtained from NENA by contacting the Committee Resource Manager identified on NENA’s website at
86 [www.nena.org/ipr](http://www.nena.org/ipr).

87 Consistent with the NENA IPR Policy, available at [www.nena.org/ipr](http://www.nena.org/ipr), NENA invites any interested party to
88 bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover
89 technology that may be required to implement this document.

90 Please address the information to:

91 National Emergency Number Association
92 1700 Diagonal Rd, Suite 500
93 Alexandria, VA 22314
94 202.466.4911
95 or [commleadership@nena.org](mailto:commleadership@nena.org)

99

100 **Reason for Issue/Reissue**

101 NENA reserves the right to modify this document. Upon revision, the reason(s) will be provided in
102 the table below.

<table>
<thead>
<tr>
<th>Document Number</th>
<th>Approval Date</th>
<th>Reason For Issue/Reissue</th>
</tr>
</thead>
<tbody>
<tr>
<td>NENA 53-001</td>
<td>06/07/2005</td>
<td>Initial Document</td>
</tr>
<tr>
<td>NENA-INF-017.2-2015</td>
<td>11/12/2015</td>
<td>This document was updated and reissued by NENA to ensure content was current with industry changes and advancements made since the original issue date.</td>
</tr>
<tr>
<td>NENA-INF-017.3-201Y</td>
<td>[MM/DD/YYYY]</td>
<td>This document was updated and reissued by NENA to ensure content was current with industry changes and advancements made since the original issue date. It was also moved to the most current document template.</td>
</tr>
</tbody>
</table>
Table of Contents

1 EXECUTIVE OVERVIEW ........................................................................................................5
2 DISASTER AND CONTINGENCY PLANS .............................................................................6
  2.1 STAFFING .........................................................................................................................6
  2.2 IT SECURITY .......................................................................................................................6
  2.3 REDUNDANT AND RESILIENT SYSTEMS ........................................................................7
  2.3.1 Electrical Power and HVAC .........................................................................................8
  2.3.2 Telephone Service .........................................................................................................8
  2.3.3 Public Safety Radio Network .......................................................................................11
  2.3.4 Computer-Aided-Dispatch (CAD) .............................................................................11
  2.4 EVACUATION ....................................................................................................................11
  2.4.1 Rationale for Evacuation .............................................................................................11
  2.4.2 Uninhabitable Environment .........................................................................................11
  2.4.3 Infrastructure Failure ..................................................................................................12
  2.5 EVACUATION PRE-PLANS ..............................................................................................12
  2.6 EVACUATION PROCEDURES .........................................................................................13
  2.7 SHELTER IN PLACE-Lockdown ........................................................................................13
  2.7.1 Rationale to Shelter in Place-Lockdown ......................................................................14
  2.8 RETURN TO NORMAL OPERATIONS ............................................................................14
3 IMPACTS, CONSIDERATIONS, ABBREVIATIONS, TERMS, AND DEFINITIONS .................15
  3.1 OPERATIONS IMPACTS SUMMARY .............................................................................15
  3.2 TECHNICAL IMPACTS SUMMARY .................................................................................15
  3.3 SECURITY IMPACTS SUMMARY ....................................................................................15
  3.4 RECOMMENDATION FOR ADDITIONAL DEVELOPMENT WORK ................................15
  3.5 ANTICIPATED TIMELINE ................................................................................................15
  3.6 COST FACTORS ..............................................................................................................16
  3.7 COST RECOVERY CONSIDERATIONS .........................................................................16
  3.8 ADDITIONAL IMPACTS (NON-COST RELATED) ............................................................16
  3.9 ABBREVIATIONS, TERMS, AND DEFINITIONS .............................................................16
4 RECOMMENDED READING AND REFERENCES ................................................................19
EXHIBIT A: EVACUATION CHECKLIST (SAMPLE) ..................................................................22
EXHIBIT B: RETURN TO NORMAL OPERATIONS CHECKLIST (SAMPLE) ..............................23
EXHIBIT C: CHECKLIST FOR DENIAL OF SERVICE ATTACKS AGAINST 9-1-1 CENTERS ......24
EXHIBIT D: CONTINUITY PLAN TEMPLATE FOR NON-FEDERAL GOVERNMENTS ..............26
EXHIBIT E: EXAMPLE OF EVACUATION AND SHELTER IN PLACE DECISION TREE ...........27
1 Executive Overview

The purpose of this document is to serve as a reference to a contingency planning section of a Standard Operating Procedure (SOP) for use by Communications Centers and/or PSAP Authorities as guidance in the formulation of an agency SOP. Each agency is unique in its resources and operations and as such, this document should be modified and/or updated to meet the requirements and legal obligations of differing modes of operations.

Fulfilling the essential mission of Communications Centers/PSAP Authorities requires that daily operations continue regardless of physical, environmental or operational circumstances. It is therefore imperative that PSAPs have plans and procedures for manmade and natural circumstances that have the potential to adversely affect the ability of the staff to perform their duties, independently of the time of day.

This document includes best practices, guidelines and procedures on:

- Staffing
- IT Security
- Redundant Systems
- Situations requiring evacuation
- Evacuation Procedures
- Return to Normal Operations

Purpose and Scope

The purpose of the NENA Model Recommendation for Disaster and Contingency Plans is to provide general guidelines for circumstances that may adversely impact the Communications Center/PSAP Authorities personnel to receive, process, dispatch and monitor emergency calls for assistance.

As each agency has unique resources and circumstances, this document should be modified and/or updated to meet the individual needs of the Communications Center/PSAP Authority as required to plan for disaster operations and recovery.

Reason to Implement

Appropriate implementation of the concepts addressed in this document will enhance the Communication Center’s/PSAP Authorities ability to maintain normal operations using standardized guidelines during disaster situations.

Benefits

Implementation of this Model Recommendation as a Standard Operating Procedure will:

- Prepare Communications Centers/PSAP Authorities for disaster and recovery situations.
- Provide guidelines for the orderly evacuation of the Communications Center.
- Provide guidelines for the return to normal operations.
- Increase the probability of maintaining functionality during a disaster and recovery situation.
- Provide a model for minimum recommendations for backup operations
- Ensure a high level of IT security
Cover topics such as backup procedures for system failures with Computer Aided Dispatch, radio systems, GIS, power systems, mobile data technologies and NG9-1-1 related functions.

2 Disaster and Contingency Plans

2.1 Staffing
The PSAP Authority is responsible for determining disaster and contingency staffing levels, and ensuring that adequate levels are maintained. Adequate staffing is the number of staff needed to achieve desired service delivery during a disaster, where minimum staffing is the lowest, predetermined number of staff required per shift. These staffing levels may be constrained by the physical limitations of the back-up facility (number of positions, fire safety/occupancy limits, etc.).

PSAP Authorities should refer to their local emergency operation plans, labor contracts, state statues, Fair Labor Standards Act (FLSA), and National Incident Management System (NIMS) to assist in establishing an operational schedule for their regular and back-up communication centers. If adequate staffing levels are not being met, the PSAP Authority shall make every effort to complete staffing through the use of reassignment, overtime, part-time, or on-call personnel, who are fit for duty. PSAP Authorities should consider both internal and external resources mutual aid from other PSAPs, Telecommunicator Emergency Response Taskforce (TERT), and other civilian agencies. If off-duty personnel are not available and minimum staffing levels have not been met, then the PSAP Authority shall require that on-duty personnel remain on-duty until minimum staffing levels can be met, or employees reach the maximum number of work hours allowable.

During times of inclement weather telecommunicators should plan accordingly. This includes planning to arrive at work on time and preparing to stay for an extended time, if required.

Safe transportation should be considered, if travel conditions warrant.

Sleeping accommodations should be available for all staff staying at the Communications Center during disaster operations.

Food and comfort facilities should be available for all staff during disaster operations.

Employees are encouraged to develop a personal family emergency plan to be assured they are prepared for disasters and to assist employees to focus on work duties. Employees can refer to the TERT deployment checklist referenced in APCO/NENA ANS 1.105.2-2015 Standard for Telecommunicator Emergency Response Taskforce to help prepare to remain at work for long periods of time. Refer to http://ready.gov for additional references.

2.2 IT Security
Today’s PSAP Authorities face more cybersecurity risks and threats than ever before. From hackers to intruders, denial of service attacks, third party vendors, to inadvertent user error, PSAP Authorities must carefully protect their information technology components, by running regular vulnerability assessments and audits. The PSAP Authority should have a concise cyber plan that
includes training and awareness. ¹ The availability of a PSAP Authority can be directly impacted by any of the aforementioned threats and as such an in-depth approach to IT Security is required.

IT Security can be defined as “the protection of information systems against unauthorized access to or unauthorized modification of information whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats” [Source: Exhibit C: Checklist for Denial of Service Attacks Against 9-1-1 Centers]

Any Contingency or Disaster Recovery Plan should include appropriate IT security measures². Please refer to Technical and Operational Information Document(s) from the NENA Security Standards that addresses IT Security as it relates to the PSAP Authority in greater detail.

2.3 Redundant and Resilient Systems

Component failure is inevitable. Any issue which hinders the ability to receive, process, dispatch and monitor emergency calls must be quickly handled with none or minimal disruption. Redundant and resilient systems are needed to continue operation when a failure causes the loss or damage of a needed resource. The method of redundancy and resiliency will vary between Communications Centers/PSAP Authorities. It is desirable to have at least two layers of redundancy for each major component of the system. It is recommended that 9-1-1 systems meet at the minimum the required best practice as defined by FCC CSRIC³. It’s suggested all redundant and resilient systems should be tested for operability no less than monthly. These systems include but are not limited to:

¹ FCC-TFOPA Task Force on Optimal PSAP Architecture
² US Telecom Cybersecurity Toolkit
³ FCC-Communications Security, Reliability and Interoperability Council- Best Practices Search Tool
2.3.1 **Electrical Power and HVAC**

2.3.1.1 The Communications Center will have at least one back-up generator with the capacity to operate automatically all critical and essential components of the system and Communications Center, including HVAC (heating, ventilation, and air conditioning).

2.3.1.2 All console equipment and radio equipment shall be connected to UPS (Uninterruptible Power Supply). Local or centralized.

2.3.1.3 Back-up power supply will have the ability to run indefinitely so long as fuel is available.

2.3.1.4 Agreements should be in place with a fueling facility, to include 24/7 delivery and contact information. **Attention must be given to how fuel will be delivered if normal transportation routes are impacted by a local disaster.** Fuel truck drivers must have credentials that permit them to pass through lawful checkpoints as needed.

2.3.1.5 Regular maintenance and testing should be done on both the generator and UPS to ensure functionality during a power loss.

2.3.2 **Telephone Service**

To meet the minimum requirements that are set in other NENA standards as it relates to resiliency, redundancy and diversity as defined in NENA 03-501, NENA Technical Information Document on Network Quality Assurance [16].

2.3.2.1 The Communications Center shall have a procedure to reroute non-emergency and emergency phone calls in the event of a failure of the primary phone system. This may be accomplished by several means:

- Network control which directs calls to back-up numbers. These numbers may terminate at the console or at a secondary site.

- Transfer calls to an alternate PSAP Authority. The alternate PSAP Authority can be another jurisdiction or a back-up facility. PSAP Authorities should consider any local, state and/or federal standards or legislation in determining re-routing procedures.

- In an E9-1-1 environment PSAP Authorities should where feasible geo-diversify their connections and routing of phone lines, as well as end offices serving the PSAP.

- In a NG9-1-1 environment, the agency could provision a method of remotely accessing their network via an alternate broadband connection.

---

4 FCC CSRIC Best Practices number 9-9-3238
• In a NG9-1-1 environment utilizing hosted solutions, PSAP Authorities should ensure geo diversity and multiple remote host capability.

• Policy Routing Rules for 9-1-1 calls only in a NG9-1-1 environment need to be pre-determined. [NENA-STA-003 NENA Standard for NG9-1-1 Policy Routing Rules]

• The Communications Center should develop a procedure to notify the back-up jurisdiction or facility before calls are rerouted (e.g.: radio channel).

2.3.2.2 PSAP Authorities may register to have priority access for communication services and restoration during an emergency. Here are some of the services available:

• **Priority Communications Services** - Getting calls through during an emergency or major disaster is essential for 9-1-1 call centers, police, fire, EMS, healthcare providers, critical infrastructure providers, and key leaders to carry out their duties. The Federal government has three excellent priority communications programs in place to help ensure that these vital calls get through the network and that telecommunications services are restored or added on a priority basis. These programs should be an important aspect of any communications reliability strategy especially for those who rely on telecommunications services to effectively respond to emergencies on a daily basis. These programs provide national security and emergency preparedness services that should be used in an emergency.

• **Telecommunications Service Priority (TSP)** - an FCC program that directs telecommunications service providers (e.g., wireline and wireless phone companies) to give preferential treatment to users enrolled in the program when they need to add new lines or have their lines restored following a disruption of service, regardless of the cause. Designated lines and circuits must be preregistered for priority restoration.

• **Government Emergency Telecommunications Service (GETS)** - a Federal program that prioritizes calls over wireline networks. Users receive an access card (GETS card), which has both the universal GETS access number and a Personal Identification Number (PIN).

• **Wireless Priority Service (WPS)** – a Federal program that prioritizes calls over wireless networks. Once the wireless device is enrolled in WPS, users dial a special access number to receive calling queue priority.

• **Dedicated National Public Safety Broadband Network (NPSBN)** – PSAP Authorities have the ability to subscribe to a dedicated broadband network for wireless and data communications.
2.3.2.3 The Communications Center shall have access to the appropriate emergency alerting system(s) to notify citizens in the event that access to 9-1-1 is compromised or unavailable. Examples can be found below in section 3.3.2.6. The notifications shall have procedures for reporting emergencies. Factors to consider include:

- PSAP Authorities might consider having additional landline and wireless phones available to PSAP staff to use during an emergency;
- PSAP Authorities should routinely test 10-digit emergency numbers to ensure they remain operational;
- PSAP Authorities need to factor in how they will adhere to Americans with Disability Act (ADA) requirements to receive and handle calls using Telecommunications Devices for the Deaf (TDD) when evacuating and operating from a backup facility;
- PSAP Authorities need to plan how they will continue to communicate with neighboring agencies during emergencies.

2.3.2.4 Text to 9-1-1 during an emergency

- PSAP Authorities not accepting text to 9-1-1
  - PSAP Authority should consider how they will communicate with the deaf, deaf-blind, late deafened, hard of hearing or individuals with speech disabilities during an emergency.
- PSAP Authorities accepting text to 9-1-1
  - Alternate routing of text calls should be considered during emergencies.

Source: [NENA-INF-007 NENA Information Document for Handling Text-to-9-1-1 in the PSAP]

2.3.2.5 Community Communication Social Networks/Social Media

PSAP Authorities might consider the use of social networks and social media to communicate and direct the public during an emergency. Social network and social media accounts should be set up in advance. This allows PSAP Authorities or their local government time to develop a following and educate the public and establish them as a timely and credible information source. PSAP Authorities might consider the use of a Social Media Manager or designated spokesperson to facilitate the message being put out to the community.

PSAP Authority and/or City/County Websites and Apps can be a resource to relay information to the community.

2.3.2.6 Emergency Notification Systems (ENS)

This is the general category for any communication systems used to notify persons of an emergency. These may include software applications, changeable message signs, sirens, telephone and other media.

- Integrated Public Alert & Warning System (IPAWS)/Emergency Alert System (EAS)
2.3.3 Public Safety Radio Network

PSAP Authorities should develop a contingency plan for all levels of potential failures that could occur on their entire radio network. Those plans should include evaluating any potential failure or risks for all circuits and system components that could potentially impact service to the system. This should also include redundant and hardened systems at remote communication sites, such as radio towers.

The Communications Center shall have a means of alerting and communicating with partner emergency responders in the event of a failure of the public safety radio network.

The radio contingency plans should be readily available and routinely tested to ensure operational functionality.

2.3.4 Computer-Aided-Dispatch (CAD)

The Communications Center shall have an alternative procedure to maintain operations in the event that the main Computer-Aided-Dispatch system fails.

The Communications Center shall train on the backup procedure to ensure dispatch staff is familiar and comfortable with the process.

The Communications Center should put in place a resilient CAD system with dual core systems where possible.

2.4 Evacuation

PSAP Authorities may need to evacuate for the safety of their personnel, or due to infrastructure failure. If the circumstances allow and the primary infrastructure is intact it is desirable to be used during evacuation. PSAP Authorities should develop a protocol for what situations or events that trigger an evacuation of their center. The protocol may need to be a tiered response due to PSAP Authority size and operational issues. Source: [APCO/NENA ANS 1.102.2-2010: Public Safety Answering Point (PSAP)-Service Capability Criteria Rating Scale.]

2.4.1 Rationale for Evacuation

Relocation of personnel may be required for many specific reasons. The two main factors requiring evacuation of the PSAP Authority are:

- Uninhabitable environment
- Infrastructure failure

2.4.2 Uninhabitable Environment

Situations which make the Communications Center unsafe for personnel to continue daily operations may include but are not limited to:
2.4.3 Infrastructure Failure
Situations during which technical components of the system fail – within or leading to the
Communications Center may include but are not limited to:
- Phone service outage or CPE failure
- Radio component damage
- Power failure (including backup generator)

2.5 Evacuation Pre-Plans
PSAP Authorities should review the risks and hazards that could impact their normal operations to
develop an evacuation plan for their Communication Center. Evacuation plans could vary due to
environmental issues such as hurricanes, tornadoes, wildfires, flooding and earthquakes. Each PSAP
Authority, due to their location and environment, has a set of unique factors that should be
considered during pre-planning.
In developing your pre-plans here are examples to consider:
- Identify a backup strategy that is capable of meeting your agency’s specific needs. Is it
  manned, or does staff need to travel there?
- Feasibility and rapidity to get to your backup center.
- Will your employees be able to get to your backup center from their homes?
- What do you do if your routes of travel are impeded?
- Automatic transition of your core applications to your backup facility, i.e. phone software,
  CAD.
- Maintaining your emergency communication during the evacuation using automated 9-1-1
  re-route and manning radio channels.

You may need to develop a multi-tiered plan to attempt to factor all the variables that could occur
during a disaster. Your pre-plan should have trigger points that dictate what events would activate
certain actions. The NENA-INF-019.2.2016 Hazard and Vulnerability Analysis document should be
used as reference when developing your PSAP evacuation pre-plans.
2.6 Evacuation Procedures

The Director or Designee shall have the authority to activate all or any part of the Disaster and Contingency Plan.

Evacuation procedures and duties must be adapted to the individual circumstances of the implementing agency. PSAP Authorities should establish procedures which provide for a quick and seamless as possible transfer of critical operations from one location to another. Redundancy within your infrastructure should be considered to limit the tasks to be completed during an evacuation. Intermediate evacuation steps, such as a mobile communications vehicle with phone and radio communications to maintain operations, until the backup site is staffed will enhance the system and maintain service.

Examples of tasks that may need to be done when evacuating:
- Notify all duty staff to respond to alternate site
- Notify your Communication Service Provider and/or 9-1-1 System Service Provider (911SSP) and when appropriate activate contingency routing of emergency and non-emergency phone calls. Ensure that routing includes both 9-1-1 trunks and other emergency and non-emergency lines. (consider automation)
- Notify database providers
- Notify radio contractor
- Ensure alternate PSAP Authority is staffed/notified of evacuation
- Notify other PSAP Authorities of evacuation and termination of direct lines
- Alternate Route Law Enforcement Terminals
- Notify all agencies, service providers and emergency responders that could be impacted by the evacuation
- Ensure the evacuation of all staff
- Confirm routing of emergency and non-emergency calls as noted in Telephone Services 3.3.2
- Confirm the ability to communicate with emergency responders.

2.7 Shelter in Place-Lockdown

Shelter in place is the use of the structure and its indoor atmosphere to temporarily separate individuals from a hazardous outdoor environment. Hazardous environment can include weather related events, bio-hazards, pandemic, threat to the safety of the center personnel, or structure. PSAP Authorities should do an assessment on their center to ensure employees can safely shelter in place during these types of events.

Lockdown may be required when employees need to seek refuge from violence, by closing a door or barricading a door. PSAP Authorities should provide guidance in advance to assist employees and
management in evaluating events to decide the most appropriate course of action; evacuation, shelter in place or lockdown.

2.7.1 Rationale to Shelter in Place-Lockdown

PSAP Authorities may choose to shelter in place under certain situations where the ability to maintain operations would be less impacted and/or it is unsafe for personnel to leave. PSAP Authorities should develop a pre-plan for the type of incidents that would trigger the center to shelter in place. Those preplans should include who has the authority to implement the plan and the notification procedure. The NENA-INF-019.2.2016 Hazard and Vulnerability Analysis document should be used as reference when developing your PSAP shelter in place/lockdown pre-plans.

2.8 Return to Normal Operations

Prior to a return to normal operations; the Communications Center should be thoroughly assessed to ensure that it is safe for personnel to return. If the event was an infrastructure incident then all technical contractors should assess their equipment for operational functionality. When the Communications Center has been assessed and all components found to be in normal working order the authorization to return to normal operations will be given.

Return to normal operations procedures and duties must be adapted to the individual circumstances of the implementing agency. PSAP Authorities shall establish procedures which provide for a quick transfer of operations from one location to another. Intermediate relocation steps such as a mobile communications vehicle with phone and radio communications to maintain operations until the primary site is staffed and ready will enhance the system and maintain service.

- Examples of tasks that may need to be done to resume normal operations. PSAP Authorities pre-plan should designate duty responsibility and delegation. Notify designated staff to return to Communications Center
- Ensure staffing of a back-up site until the Communications Center is prepared to resume normal operations
- Notify CSP and/or 911SSP and when appropriate activate normal routing of 9-1-1 trunks and other emergency phone lines
- Notify database providers
- Notify radio contractor
- Notify other PSAP Authorities of return to normal operations and resumption of direct lines
- Reverse alternate routing of Law Enforcement Terminals
- Ensure all agencies, service providers and emergency responders are notified
- Ensure all personnel are accounted for
- Confirm routing of emergency calls and ability to communicate with emergency responders
3 Impacts, Considerations, Abbreviations, Terms, and Definitions

3.1 Operations Impacts Summary

PSAP authorities should consider risk, disaster and contingency plans to assure continuity of operations. This document is intended as guideline to a PSAP manager. PSAP adoption of this standard calls for local staff to assume task responsibility for evaluation, implementation and compliance with all elements of the standard. Such tasks should include performing a hazard, vulnerability and risk assessment analysis of facilities, infrastructure, plans and resources. Additionally, tasks and responsibilities may include procuring funding for the PSAP authority.

APCO/NENAANS 1.102.2-2010: Public Safety Answering Point (PSAP)-Service Capability Criteria Rating Scale, assists PSAP managers and their governing authorities to identify their current level of service capability. An assessment tool is provided to facilitate an objective review of the current capabilities of the PSAP Authority against models representing the best level of preparedness, survivability and sustainability amidst a wide range of natural and man-made events.

The self-evaluation assessment tool is also intended to provide the basis for discussion with funding bodies (federal, state, county, municipal, etc.) concerning the PSAP Authority status in regard to their current technological position, and readiness or effectiveness to survive certain risks associated with local vulnerabilities.

3.2 Technical Impacts Summary

In the event of an evacuation of the Communications Center/PSAP Authority, alternate means of call reception, data entry and retention, dispatch and monitoring must be available. The technical impact will vary greatly dependent upon the size and complexity of the emergency call center. At a minimum the Communication Service Provider (referred to in the past as the “Telephone Company or Telephone Service Provider”), 9-1-1 System Service Provider (911SSP), radio, IT personnel, Computer-Aided-Dispatch vendor and any other service provider or vendor unique to the agency should be consulted to review options for alternate call taking and dispatching services.

3.3 Security Impacts Summary

PSAPs should consider security impacts on technical and operational issues to comply with current NENA documents when implementing their disaster, recovery and contingency plans. PSAP Authorities should take into consideration any internal, local, state and federal recommendations and/or legal requirements.

3.4 Recommendation for Additional Development Work

No additional work is recommended at this time.

3.5 Anticipated Timeline

The anticipated timeline will vary depending on the size and complexity of the operational and technical requirements of the Communications Center.
3.6 Cost Factors

It is recommended that a back-up solution be adequate to meet the basic needs of the systems. It need not be a fully redundant, mirror of the primary Communications Center, unless otherwise required by local or state law. A backup solution could be a facility, ad-hoc or virtual in nature. The cost of this recommendation will vary greatly depending on the size and complexity of the systems. Costs could include reoccurring and nonrecurring expenses, which will likewise be dependent upon the systems. Wherever feasible, a back-up solution should be scalable and multi-use. An example of dual use is a back-up solution that is also used for Telecommunicator training.

3.7 Cost Recovery Considerations

Cost Recovery will vary greatly depending on the jurisdiction of the Communication Center/PSAP Authority Administrators are encouraged to review their cost recovery legislation and apply for all available grant and/or funding.

3.8 Additional Impacts (non-cost related)

Based on the analysis of the authoring group, the information or requirements contained in this NENA document are known to have several impacts. The primary impacts may be borne by an agency at no additional cost if an existing employee is tasked with these responsibilities and training, testing, review and drills are conducted during already scheduled in-service training. Otherwise yes there will be a cost associated with these things. The primary impacts include:

a. Planning and preparation of operational and technical needs
b. Staff training and drills
c. Routine testing of equipment
d. Development and review of After Action Reports
e. Regular review of the risk/disaster/contingency plan
f. Implement changes to risk/disaster/contingency plans as required

3.9 Abbreviations, Terms, and Definitions

See NENA Master Glossary of 9-1-1 Terminology, NENA-ADM-000 [1], for a complete listing of terms used in NENA documents. All abbreviations used in this document are listed below, along with any new or updated terms and definitions.

<table>
<thead>
<tr>
<th>Term or Abbreviation (Expansion)</th>
<th>Definition / Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WG Recommendations for Master Glossary: (THIS COLUMN WILL BE DELETED BEFORE PUBLICATION)</td>
<td></td>
</tr>
<tr>
<td>(OK)Master Glossary Reviewed &amp; Accepted</td>
<td></td>
</tr>
<tr>
<td>(A)dd</td>
<td></td>
</tr>
</tbody>
</table>

[MM/DD/YYYY]
| **ENS (Emergency Notification Systems)** | General category for any systems used to notify persons of an emergency. May include changeable message signs, sirens, telephone and other media. |
| **CSP (Communications Service Provider)** | This term is used generically to refer to any and all providers of telecommunications services that may be used to generate a 9-1-1 call, and who would interconnect in any fashion to the 9-1-1 network. CSP include wireline ILECS and CLECs, Wireless Service Providers, VoIP Service Providers, operators of large PBXs and any other entity providing telecommunications services to the general public. |
| **IPAWS (Integrated Public Alert Warning System)** | A modernization and integration of the nation’s alert and warning infrastructure, Federal, State, local, tribal and territorial alerting authorities can use IPAWS and integrate local systems that use Common Alerting Protocol standards with the IPAWS infrastructure. IPAWS provides public safety officials with an effective way to alert and warn the public about serious emergencies using the Emergency Alert System (EAS), Wireless Emergency Alerts (WEA), the National Oceanic and Atmospheric Administration (NOAA) Weather Radio, and other public alerting systems from a single interface. [https://www.fema.gov/integrated-public-alert-warning-system](https://www.fema.gov/integrated-public-alert-warning-system) |
| **NIMS (National Incident Management System)** | A systematic, proactive approach to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sector to work together seamlessly and manage incidents involving all threats and hazards—regardless of cause, size, location, or complexity—in order to reduce loss of life, property and harm to the environment. The NIMS is the essential foundation to the National Preparedness System (NPS) and provides the template for the management of incidents and operations in support of all five National Planning Frameworks. Use the images below for direct links to all pages within the NIMS website. [http://www.fema.gov/national-incident-management-system](http://www.fema.gov/national-incident-management-system) |
| **NG9-1-1 (Next Generation 9-1-1)** | NG9-1-1 is an Internet Protocol (IP)-based system comprised of managed Emergency Services IP networks (ESInets), functional elements (applications), and databases that replicate traditional E9-1-1 features and functions and provides additional capabilities. NG9-1-1 is designed to provide access to emergency services from all connected communications sources, and provide multimedia data capabilities for Public Safety Answering Points (PSAPs) and other emergency service organizations. |
| **PSAP (Public Safety Answering Point)** | An entity responsible for receiving 9-1-1 calls and processing those calls according to a specific operational policy. |
| **SOP (Standard Operating Procedure)** | A written directive that provides a guideline for carrying out an activity. The guideline may be made mandatory by including terms such as “shall” rather than “should” or “must” rather than “may”. |
| **TERT (Telecommunicator Emergency Response Taskforce)** | A group of trained telecommunications operations and support personnel able to respond to and work with another agency to receive, process, dispatch and monitor calls for assistance. [http://www.njti-tert.org/](http://www.njti-tert.org/) |
**Recommended Reading and References**

This is a list of the documents and web sites referenced and used in the development of this NENA standard document.

1. NENA-ADM-000, NENA Master Glossary of 9 1 1 Terminology
2. NENA-INF-019.2.2016, NENA Hazard and Vulnerability Analysis Information Document
3. NENA-INF-020.2.2017, NENA PSAP Survivability Information Document
4. APCO/NENA ANSI.1.105.2-2015 Standard for Telecommunicator Emergency Response Taskforce (TERT) Deployment
6. NENA 75-001, NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)
7. NENA 75-502, NENA Next Generation 9-1-1 (NG-SEC) Audit Checklist
9. US Telecom Cyber Security Toolkit
10. NIST Cybersecurity Framework
12. FCC Priority Communication Services
13. FCC Telecommunications Service Priority (TSP)
14. FCC Government Emergency Telecommunications Service (GETS)
15. FCC Wireless Priority Service (WPS)
Text to 9-1-1

[17] NENA SMS Text to 9-1-1 Resources for PSAP’s & 9-1-1 Authorities
[18] NENA-INF-007, NENA Information Document for Handling Text Message Calls to 9-1-1 in the PSAP
[19] NENA SMS Text to 9-1-1 Information and Planning Guide
[22] NENA 53-504, NENA Drills and Exercises Operations Information Document
[23] NENA-STA-009, NENA Mutual Aid Standard/Model Recommendation
[25] NENA 56-506, NENA Public Safety Answering Point Site Selection Criteria
[26] APCO/NENA.ANS 1.102.1-2010 Public Safety Answering Point (PSAP)-Service Capability Criteria Rating Scale

Training

[27] NENA “Preparing for the Worst” courses (continuity and disaster planning). http://www.nena.org/?page=PrepareWorstCourses

Continuity Planning


[MM/DD/YYYY]
Shelter in Place – Lockdown – Evacuation


[39] Run-Hide or Fight DHS Video: https://www.youtube.com/watch?v=5VcSwejU2D0

[40] Center for Disease Control and Prevention – Learn how to shelter in place
http://emergency.cdc.gov/preparedness/shelter/
Exhibit A: Evacuation checklist (sample)

Example On-Duty Supervisor/Telecommunicator Duties

- Off Duty Staff notified (Page group)
- Priority Radio and MDT message
- 911SSP Special Circuits (XXX) XXX-XXXX notify only
- Communications Service Provider (CSP) (telephone service)
- Radio Contractor (XXX) XXX-XXXX (Page Group)
- ARES/RACES (Page Group)
- Other County PSAP Authorities
- Local Emergency Management (such as municipal, county and/or parish)
- State Emergency Management
- Law Enforcement Terminal (Alt. Route to XXXXXX)
- Remote Site Operational
- Contingency route 9-1-1 and emergency lines
- Relocate unassigned personnel
- Account for personnel

Example Director/Manager Duties

- Commissioners/Staff Notified
- Supervisors Checklist reviewed
- Technician response
- Administrative staff response
- PIO response
- Remote sites notified/staffed/operational
- Radios/pagers tested
- Law Enforcement terminal forwarded
- Contingency call routing directed
- Staff Accounted for and assigned

Example of IT Personnel Duties

- Technical staff responding
- Radio Techs responding
- Phone Techs responding
- Radios operational
- Phones Operational
- Pagers operational
- IP Connectivity
- Contingency routing directed (Director)
Exhibit B: Return to normal operations checklist (sample)

Example On Duty Supervisor/Telecommunicator Duties

______ Assign staff to return to Communications Center
______ Priority Radio canceled and MDT message
______ 911SSP Special Circuits (XXX) XXX-XXXX notify only
______ Communications Service Provider (CSP) (telephone service)
______ Radio Contractor (XXX) XXX-XXXX
______ ARES/RACES
______ Other County PSAP Authorities
______ Local Emergency Management (such as municipal, county and/or parish)
______ State Emergency Management
______ Law Enforcement Terminal (Reverse Alt. Route to XXXXXXX)
______ Cancel contingency routing of 9-1-1 and emergency lines
______ Release unassigned personnel
______ Account for on duty personnel

Example Director/Manager Duties

______ Ensure safety of Communications Center
______ Technical Manager ensures system operational
______ Commissioners/Staff Notified
______ Supervisors Checklist reviewed
______ Communications Center notified/staffed/operational
______ Radios/pagers tested
______ Reverse Law Enforcement Terminal Alternate Routing
______ Cancel contingency call routing directed
______ Staff Accounted for and assigned or released
______ Remote site re-supplied and operational
______ After-action report completed

Example IT Personnel Duties

______ All systems operational
______ Notify Director that Communications Center Operational
______ Release technicians

Commentary:

Checklists provide guidelines for tasks that must be completed. Each Communications Center/PSAP Authority should develop checklist unique to their circumstances for evacuation and (pre and post) return to normal operations.
Exhibit C: Checklist for Denial of Service Attacks Against 9-1-1 Centers

Information continues to be received from multiple jurisdictions indicating the existence of ongoing attacks targeting the telephone systems of public sector entities. Over 200 such attacks have been identified to date. The perpetrators of the attack launched numerous phone calls against the target telephone network, tying up the system and preventing the agency from receiving legitimate calls. This type of attack is referred to as a TDoS or Telephony Denial of Service Attack.

As a result of a cooperative effort between Federal Authorities, public safety representatives, and commercial service providers, the following checklist has been developed to provide you with information that will assist in the development of a continuity of operations plan for your agency.

1. **Before a TDoS Event**
   a. Discuss how to respond to a TDoS event with your service provider. These discussions might include both your telephone service providers (9-1-1 and Administrative phones - if separate providers) as well as your 9-1-1 Equipment vendors.
   b. Ensure that the Public Safety Telecommunicators and their supervisors have access to the phone number and direct contact information for the service provider’s personnel or division equipped to respond to a public safety TDoS.
   c. Discuss with your telephone system engineer or technician possible configuration changes to isolate critical phone lines (incoming 9-1-1 calls for service) from administrative and other lines, taking into account hunt-groups, busy or no-answer rollover to other lines, rollover to other PSAP Authorities, etc. Prevent an overload of non-critical lines from rolling-over to lines answered by 9-1-1 call-takers
   d. Remind employees of their obligations to protect personally identifying information, and how to protect themselves from identity theft (Federal Trade Commission, Consumer Information for an example). Additionally, if an attack were to occur at your agency reassure the targeted employee that they are not responsible for the attack. They and the center are merely victims of a highly sophisticated criminal enterprise.

2. **During a TDoS Event**
   a. Save the voice recording of suspects who may call before, during or after the TDoS events.
   b. Record all phone numbers and account information, if the caller is demanding payment(s):
      i. Start and stop times of the events
      ii. number of calls per hour or per day
      iii. phone numbers and other ANI/ALI information of the incoming calls
      iv. IP addresses if applicable
v. Any instructions for how to pay, such as account number, call-back phone number etc.

c. Retain all call logs and IP Logs

d. Attempt to separate the affected phone number from 9-1-1 and other critical trunks – work with your PBX provider/maintainer.

3. **After a TDoS Event**

a. File a complaint with the [Internet Crime Complaint Center](https://www.ic3.gov) - co-sponsored by the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C).

Include the keywords **TDoS, PSAP, and Public Safety** in the description of the incident.

b. File a report with your local police department or sheriff’s office.

i. If the investigator is unsure of how to proceed there are resources available to assist. The FBI, FCC (Federal Communications Commission) and FTC (Federal Trade Commission) are all engaged in this process, and DHS-NCC-NCCIC (Department of Homeland Security - National Coordinating Center for Communications - National Cybersecurity and Communications Integration Center) can help coordinate information.

ii. Advise them that the CALEA (Communications Assistance for Law Enforcement Act) protocol can be invoked, enabling service providers to collect data on the originator of the call and provide it to law enforcement resources.

c. Consolidate call logs and IP logs; mark for long-term retention.

9-1-1 Centers / PSAP Authorities should also make efforts to share this information with other public safety facilities with which they interact including: private ambulance service dispatch centers, hospitals, air ambulance dispatch centers etc.

---

NENA NG9-1-1 Security Information Document, NENA-INF-015.1-2016, as indicated in section 3.8 “Avoiding DoS/TDoS is currently not possible. Such attacks should be considered “when”, not “if”. Network planners should utilize NENA 75-502, NG-SEC Audit Checklist.”
Exhibit D: **Continuity Plan Template for Non-Federal Governments**

This FEMA template provides instructions, guidance and sample text for the development of continuity plans and programs.
Exhibit E: Example of Evacuation and Shelter in Place Decision Tree

Event
- Event requiring PSAP to consider whether evacuation or Shelter in Place (SIP) plans should be activated
- External and internal intelligence regarding event

Must Shelter-in-Place
- The external environment would pose a greater danger to staff and visitors than evacuation (e.g., chemical/biological agent release, nuclear incident plume, civil unrest/hostility)
- Adequate and timely facility and/or mutual aid resources are not available or accessible (e.g., earthquake)

Must Evacuate
- The proximity, scope and/or expected duration of event poses an immediate threat to staff safety
- Adequate and timely facility and/or mutual aid resources are available or accessible to support Full or Partial evacuation

Shelter in Place or Evacuation Decision
- Duration and scope of threat to PSAP clear but may evolve
- PSAP capabilities adequate to support normal operations with available support for estimated event duration
- May or may not be barriers mutual aid resources should evacuation become necessary

Need to Implement Reduction Measures
- PSAP capabilities not adequate to maintain full operations for estimated duration of event
- Determination made that reduction measures necessary (for example, conservation of resources, curtailment of services and/or partial PSAP evacuation)
- No identified barriers to mutual aid resources

PSAP Capabilities may include communication, resources (supplies and equipment), utilities, staff, food, water, safety and security (including safety of facilities).

Adapted from Loma Linda University Health Evacuation and Shelter In Place Decision Tree
ACKNOWLEDGEMENTS


NENA Board of Directors Approval Date: [MM/DD/YYYY] (Will be added by the CRM.)

NENA recognizes the following industry experts and their employers for their contributions to the development of this document.

<table>
<thead>
<tr>
<th>Members</th>
<th>Employer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wendi Lively ENP – PSAP Operations Committee Co-Chair</td>
<td>Spartanburg County SC</td>
</tr>
<tr>
<td>April Heinz ENP – PSAP Operations Committee Co-Chair</td>
<td>INdigital Telecom</td>
</tr>
<tr>
<td>Terri Costello RPL – WG Co-Chair</td>
<td>E-Com 9-1-1 Dispatch Homewood, IL</td>
</tr>
<tr>
<td>Cheryl LeSage ENP – WG Co-Chair</td>
<td>Fremont Police Department CA</td>
</tr>
<tr>
<td>Rick Erickson ENP</td>
<td>The Woodlands Township TX</td>
</tr>
<tr>
<td>Robert Leathers ENP</td>
<td>McLennan County 9-1-1 Emergency Assistance District TX</td>
</tr>
<tr>
<td>Bernard Brabant</td>
<td>Consultant</td>
</tr>
<tr>
<td>Pierce Power</td>
<td>Teleira</td>
</tr>
<tr>
<td>Steve Haberman</td>
<td>Mission Critical Partners Inc.</td>
</tr>
<tr>
<td>Robert Morris, ENP</td>
<td>Frontier Communications</td>
</tr>
<tr>
<td>Eddie Lemaire</td>
<td>Comtech Telecommunications Corporation</td>
</tr>
<tr>
<td>Robert Kujawa</td>
<td>Northbrook Police Department, IL</td>
</tr>
<tr>
<td>Christopher Rowe</td>
<td>Northwest CT Public Safety Communication Center</td>
</tr>
<tr>
<td>George Long</td>
<td>Willamette Valley Communication Center</td>
</tr>
<tr>
<td>Mickey Dunnavant</td>
<td>Crisp County GA</td>
</tr>
</tbody>
</table>

Special Acknowledgements:

Delaine Arnold, ENP, Committee Resource Manager, has facilitated the production of this document through the prescribed approval process.

The Contingency Planning Document Review Working Group is part of the NENA Development Group that is led by:
- Pete Eggimann, ENP, and Jim Shepard, ENP, Development Steering Council Co-Chairs
- Roger Hixson, ENP, Technical Issues Director
- Chris Carver, ENP, PSAP Operations Director