<<Insert Agency Name Here>>

Emergency Operations Plan

<<INSERT AGENCY LOGO HERE>>

**Last Revised: November 9, 2021**

**Version 1.0**

[Approval and Implementation 1](#_Toc85625854)

[Record of Changes and Distribution 2](#_Toc85625855)

[Basic Plan 3](#_Toc85625856)

[Introduction 3](#_Toc85625857)

[Purpose 4](#_Toc85625858)

[Scope 5](#_Toc85625859)

[Situation 6](#_Toc85625860)

[Staffing 6](#_Toc85625861)

[Building Information 6](#_Toc85625862)

[Service Coverage Area 6](#_Toc85625863)

[Threat, Hazard, and Vulnerability Analysis Summary 7](#_Toc85625864)

[Planning Assumptions 8](#_Toc85625865)

[Assumptions 8](#_Toc85625866)

[Limitations 8](#_Toc85625867)

[Concept of Operations 9](#_Toc85625868)

[Plan Activation 9](#_Toc85625869)

[Phases of Emergency Management 9](#_Toc85625870)

[Organization and Assignment of Responsibilities 10](#_Toc85625871)

[Organization 11](#_Toc85625872)

[Direction, Control, and Coordination 12](#_Toc85625873)

[National Incident Management System 12](#_Toc85625874)

[Incident Command System 12](#_Toc85625875)

[Transfer of Command 12](#_Toc85625876)

[Incident Coordination and/or Response Locations/Facilities 13](#_Toc85625877)

[Line of Succession 13](#_Toc85625878)

[Information Collection, Analysis, and Dissemination 14](#_Toc85625879)

[Situational Awareness 14](#_Toc85625880)

[Information Collection 14](#_Toc85625881)

[Information Analysis 14](#_Toc85625882)

[Situation Reports (SitReps) 14](#_Toc85625883)

[Public Messaging 16](#_Toc85625884)

[Communications 16](#_Toc85625885)

[Alert and Notification 17](#_Toc85625886)

[Notification of Key Officials 17](#_Toc85625887)

[Public Information Officer 17](#_Toc85625888)

[Administration, Finance, and Logistics 17](#_Toc85625889)

[Finance and Administration 17](#_Toc85625890)

[Recordkeeping 18](#_Toc85625891)

[Preservation of Records 18](#_Toc85625892)

[Reports 18](#_Toc85625893)

[Resource Management 18](#_Toc85625894)

[Mutual Aid 19](#_Toc85625895)

[Training and Exercise Program 20](#_Toc85625896)

[Training Program 20](#_Toc85625897)

[Exercise Program 21](#_Toc85625898)

[Plan Development and Maintenance 23](#_Toc85625899)

[References 24](#_Toc85625900)

[1. Functional Annexes 1-1](#_Toc85625901)

[2. Annex – Continuity of Operations Plan 2-1](#_Toc85625902)

[3. Annex – Evacuation Plan 3-1](#_Toc85625903)

[4. Annex – Site Map 4-1](#_Toc85625904)

[5. Annex – Critical Infrastructure Shutoff Locations 5-1](#_Toc85625905)

[6. Annex – Radio Communications (ICS-217, QC-II, and DTMF Tones) 6-1](#_Toc85625906)

[7. Annex – Emergency Onboarding of PSAP into <<INSERT AGENCY ACRONYM HERE>> 7-1](#_Toc85625907)

[8. Annex – Document Templates 8-1](#_Toc85625908)

[A. Hazard- and Threat-Specific Annexes A-1](#_Toc85625909)

[B. Annex – Threat/Actual Violence at or Near Workplace Plan B-1](#_Toc85625910)

[C. Annex – Cybersecurity Incident Handling Plan C-1](#_Toc85625911)

[D. Annex – Public Health Emergency D-1](#_Toc85625912)

# Approval and Implementation

This Emergency Operations Plan (EOP) for <<INSERT AGENCY ACRONYM HERE>> will become effective and considered approved upon signing by the <<INSERT AGENCY ACRONYM HERE>> Director. When approved, this plan will supersede all previous plans for emergency management.

The Director authorizes the Deputy Director to make all necessary modifications to this plan without the express written approval of the Director. These modifications must be recorded in the Record of Changes section of this plan.

<<Insert Agency Official Name Here>>

<<Insert Agency Name Here>>

# Record of Changes and Distribution

Any approved additions or modifications to this Emergency Operations Plan (EOP) will be documented and noted in this section. The date of the change, the title of the person making the change, and a summary and reason for the modifications, will be inserted into this section of the plan.

After any modification to this plan, the Emergency Management Coordinator will ensure that the updated version is distributed to the following locations and/or individuals:

* **<<IDENTIFY WHO/WHERE COPIES OF THE PLAN WILL RESIDE>>**

Personnel with a role in executive leadership, coordination and management, and operational implementation of emergency procedures are encouraged to have digital access to this plan or a printed copy of this plan available to them at all times.

| **Change Number** | **Date of Change** | **Sections** | **Summary of Change** | **Change Made By (Title or Name)** |
| --- | --- | --- | --- | --- |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |

# Basic Plan

# Introduction

To guide response activities and ensure effective and efficient coordination, <<INSERT AGENCY NAME HERE>> (<<INSERT AGENCY ACRONYM HERE>>) has developed this Emergency Operations Plan (EOP). The EOP defines the scope of preparedness and emergency management activities for <<INSERT AGENCY ACRONYM HERE>>, and facilitates all-hazard preparedness, mitigation, response, and short-term recovery activities, thereby setting the stage for a successful long-term recovery. The <<INSERT AGENCY ACRONYM HERE>> EOP describes the center’s emergency management organization, including the roles, responsibilities, and operations during a disaster, major emergency, or planned event. The EOP:

* Formulates policies designated to protect life and property during incidents affecting or threatening life or property within the center.
* Provides guidance for strategic thinking and decision-making as it relates to emergency operations.
* Assigns roles and responsibilities to mitigate, prepare for, respond to, and recover from incidents threatening life or property within the center.
* Officially establishes NIMS and the Incident Command System (ICS) as the organizational structure to guide activities during an emergency affecting the center.
* Identifies lines of authority and policy related to emergencies and disasters.

<<INSERT AGENCY ACRONYM HERE>> activates its EOP when the center must respond to an emergency that requires coordination and/or may require support from other local, state, and federal entities. In addition, <<INSERT AGENCY ACRONYM HERE>> may activate the EOP to coordinate multi-agency and/or multi-jurisdictional support of a pre-planned event.

The <<INSERT AGENCY ACRONYM HERE>> EOP does not supersede any departmental standard operating procedure (SOP) or responsibility for day-to-day operations. The EOP supplements but does not supplant the responsibilities or duties of any department or agency. The EOP also describes cooperation and integration of actions with other nearby centers and/or response entities. This plan is not intended to limit or restrict the initiative, judgment, or independent action required to provide appropriate and effective emergency response, disaster mitigation activities, preparedness, and recovery efforts.

The EOP is based on the Federal Response Plan (FRP), the National Response Framework (NRF), and National Preparedness Goal and is compliant with the National Incident Management System (NIMS), Incident Command System (ICS), and the Comprehensive Preparedness Guide (CPG) 101 Version 2 national standards. The EOP is also compatible with the state-level Massachusetts Comprehensive Emergency Management Plan (CEMP).

All <<INSERT AGENCY ACRONYM HERE>> employees and partner agencies should become familiar with this document to ensure the efficient and effective execution of their emergency responsibilities. While the plan can help to establish the relationships, responsibilities, and general guidelines.

# Purpose

The purpose of the <<INSERT AGENCY ACRONYM HERE>>s Emergency Operations Plan (EOP) is to identify and respond to incidents by outlining the responsibilities and duties of <<INSERT AGENCY ACRONYM HERE>> and its employees. Developing, maintaining, and exercising the plan empowers employees in an incident to act quickly and knowledgeably. In addition, the plan educates administration, supervisors, telecommunicators, and other key stakeholders on their roles and responsibilities before, during, and after an incident. This plan provides <<INSERT AGENCY ACRONYM HERE>> member communities and the public with assurances that <<INSERT AGENCY ACRONYM HERE>> has established guidelines and procedures to respond to incidents/hazards effectively.

The developed guidelines and procedures for dealing with existing and potential incidents are defined in the plan below. The basic plan and the functional and hazard-specific annexes outline an organized, systematic method to mitigate, prevent, protect against, respond to, and recover from incidents. <<INSERT AGENCY ACRONYM HERE>> employees have been trained to assess the seriousness of incidents and respond according to these established procedures and guidelines. <<INSERT AGENCY ACRONYM HERE>> regularly schedules staff training.

Lastly, developing, maintaining, and exercising the EOP helps to ensure that best practices are followed. Also, it helps to ensure that appropriate policies, procedures, or guidelines are tested, reviewed, and in place.

The EOP is intended to accomplish the following goals:

* Assign authorities and responsibilities to agencies, organizations, and individuals for carrying out specific actions during an emergency or event;
* Detail the methods and procedures to be used by designated personnel to assess emergencies and take appropriate actions to save lives and reduce injuries, prevent, or minimize damage to public and private property, and protect the environment;
* Provide a process by which emergency response personnel and local government staff can efficiently and effectively prevent, mitigate, prepare for, respond to, and recover from emergencies and disasters; and
* Identify the responsibilities of local agencies and partnering stakeholders and organizations during emergencies or events.

# Scope

This EOP outlines the expectations of staff; roles and responsibilities; direction and control systems; internal and external communications plans; training and sustainability plans; authority and references as defined by local, State, and Federal government mandates; common and specialized procedures; and specific hazard vulnerabilities and responses/recovery. Within this scope, the plan addresses two (2) different types of response scenarios:

* **Planned or Anticipated Incidents**: Incidents that can be planned for in advance such as a hurricane, a winter storm, extreme temperatures, major crowd events or VIP visits, etc., and;
* **Immediate Response Incidents**: such as a tornado, airplane crash, earthquake, fire, hazmat incident, active shooter, cyber incident, etc.

# Situation

## Staffing

<<INSERT AGENCY ACRONYM HERE>> employs approximately <<HOW MANY FTES WORK HERE>> Full Time Equivalents (FTEs). <<DESCRIBE YOUR FACILITY HERE>>

An employee roster is available at <<WHEREE>>. The roster is also located in the COOP Plan on **page 2-28**.

<<INSERT AGENCY ACRONYM HERE>> is committed to the safe evacuation of staff. Currently, there are no employees that require access or functional needs. However, employees should be cognizant that at some point employees or visitors to the center may require additional assistance if they are temporarily on crutches, wearing casts, etc.

## Building Information

<<INSERT AGENCY ACRONYM HERE>> is located on <<DESCRIBE THE GROUNDS AND CURTILAGE OF THE FACILITY HERE>>.

A map of the <<INSERT AGENCY ACRONYM HERE>> facility annotated with evacuation routes, shelter locations, fire alarm pull stations, fire hydrants, fire extinguishers, first aid kits, hazardous materials storage, and utility shutoffs is included on **page 5-2**. All employees are required to know these locations. Additionally, administrative, and supervisory employees are required to know how to operate the utility shutoffs.

## Service Coverage Area

<<INSERT AGENCY ACRONYM HERE>> is a <<DESCRIBE YOUR SERVICE AREA HERE INCLUDING WHO YOU SERVE, WHO YOU BACKUP, ETC>>.

# Threat, Hazard, and Vulnerability Analysis Summary

<<INSERT AGENCY ACRONYM HERE>> is exposed to many hazards, all of which have the potential for disrupting the center, causing casualties, and damaging or destroying public or private property.

In <<WHEN CONDUCTED>>, a planning team of staff members completed a thorough hazard analysis to identify any circumstances in the center or near the site that may present unique problems or potential risks to people or property. The interior and exterior portions of the building and the grounds have been assessed for potential hazards that may impact the site, the staff, or its visitors. Identified hazards have been assessed by risk and likelihood and ranked accordingly.

The below table briefly discusses <<INSERT AGENCY ACRONYM HERE>>’s high-priority hazards.

Impact: How serious is the risk?

**Major**

**Moderate**

**Minor**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Likelihood: What is the chance it will happen? | | | | |
|  | **Unlikely** | **Likely** | **Very Likely** |
|  | * **Earthquake** * **Dam Failure** * **Drought** * **Landslide** | * **Extreme Temperatures** * **Other Severe Weather** | * **Coastal Erosion** |
|  | * **Civil Unrest** * **Wildfire** * **Prison Escape** | * **Flooding** * **Tornado** | * **Hurricane/Tropical Storm** |
|  | * **Major Air Crash** * **Nuclear Power Plant Event** * **Tsunami** * **Public Health Emergency** * **Chemical, Biological, Radiological, and Nuclear (CBRN) Incident** * **Workplace Violence** | * **Infrastructure Failure** * **Hazard Material Accident/Spills** | * **Severe Winter Storm/Nor’easter** * **Cyber Incident** |

Any hazard could potentially cause circumstances in which normal operations are disrupted because of:

* Denial of access to a facility (such as damage to the building);
* Denial of service due to a reduced workforce (such as due to pandemic flu); and
* Denial of service due to equipment or systems failure (such as IT systems failure).

# Planning Assumptions

## Assumptions

Stating the planning assumptions allows <<INSERT AGENCY ACRONYM HERE>> to deviate from the plan if certain assumptions prove not to be true during operations. The EOP assumes:

* <<INSERT AGENCY ACRONYM HERE>> and/or the Commonwealth have effective prediction and warning systems in place allowing <<INSERT AGENCY ACRONYM HERE>> to anticipate certain emergencies that may impact <<INSERT AGENCY ACRONYM HERE>>.
* When anticipating or in response to an emergency situation, the Director is responsible for taking action, including the activation of this plan, to mitigate impacts, save lives, protect property and the environment, assist survivors, and restore essential services and facilities.
* <<INSERT AGENCY ACRONYM HERE>> administrative and supervisory employees are familiar with the EOP, understand their roles and responsibilities under the EOP, maintain appropriate plans, policies, and procedures to carry out those responsibilities and maintain a state of readiness. Day-to-day functions which do not contribute directly to the emergency operation may be suspended for the duration of an emergency/disaster. Resources that would normally be required for those daily functions will be redirected to tasks in support of the emergency response.
* <<INSERT AGENCY ACRONYM HERE>> will use its own resources in response to an emergency or disaster. Once local resources are exhausted (or near exhausted), requests for assistance will be made through <<HOW ARE REQUESTS FOR ASSISTANCE MADE>>.
* A large-scale emergency or disaster may overwhelm available local resources, leading to the need for support from local/mutual aid jurisdictions, private sector partners, state agencies, and the federal government.
* <<INSERT AGENCY ACRONYM HERE>> anticipates support from <<DESCRIBE WHO HERE>> should the resources of <<INSERT AGENCY ACRONYM HERE>> become exhausted.
* Disaster support from federal agencies may take at least 72 hours to arrive.
* Disaster support from state resources and/or local homeland security assets may take at least 4-8 hours to arrive.

## Limitations

It is the policy of <<INSERT AGENCY ACRONYM HERE>> that no guarantee is implied by this plan of a perfect incident management system. As personnel and resources may be overwhelmed, <<INSERT AGENCY ACRONYM HERE>> can only endeavor to make every reasonable effort to manage the situation, with the resources and information available at the time.

# Concept of Operations

This plan is based upon the concept that the incident management functions that must be performed by the site generally parallel some of their routine day-to-day functions. To the extent possible, the same personnel and material resources used for day-to-day activities will be employed during incidents. Because personnel and equipment resources are limited, some routine functions that do not contribute directly to the incident may be suspended. The personnel, equipment, and supplies that would typically be required for those routine functions will be redirected to accomplish assigned incident management tasks.

## Plan Activation

The EOP and its associated annexes will be executed in whole or in part as directed by Director, or other duly authorized representatives in response to an existing or an impending emergency. This plan may also be activated under the following circumstances:

* At the time of an actual disaster;
* When the <<IDENTIFY CITY/TOWN HERE>> has declared a local state of emergency;
* When the Governor of <<YOUR STATE>> has declared a State of Emergency for areas that include <<INSERT AGENCY ACRONYM HERE>>; or
* When a Presidential Declaration of an Emergency or Disaster is issued for areas that include <<INSERT AGENCY ACRONYM HERE>>.

## Phases of Emergency Management

<<INSERT AGENCY ACRONYM HERE>>’s emergency operations plan addresses all phases of emergency management for all types of incidents, including prevention and mitigation, preparedness, response, and recovery.

### Prevention and Mitigation

Prevention involves identifying preventative, corrective, or deterring measures and actions to prevent or limit bodily injury, loss of life, or property damage from disasters and emergencies. It includes consideration of policy issues as well as structural projects within the government and the private sector. Preventive measures are designed to provide more permanent protection from disasters; however, not all disasters can be prevented.

The goal of mitigation is to prevent future loss by eliminating or reducing risks. Mitigation activities link the recovery and preparedness phases in the emergency management cycle and can occur before or after an emergency. The goals of pre-emergency mitigation activities are to prevent an emergency, reduce the chance of an emergency happening, or reduce the damaging effects of unavoidable emergencies. The goal of post-emergency mitigation is to eliminate or reduce the impact of the hazards realized during the emergency. Post-emergency mitigation is part of the recovery process.

### Preparedness

Preparedness involves activities undertaken in advance of an emergency or disaster to adequately prepare for and develop the capability to respond to an emergency. Preparedness activities include planning, organizing, training equipping, exercising, evaluating, and implementing corrective actions for the emergency management program and organization.

Preparedness activities develop operational capabilities and enable an effective response to an emergency or disaster, and involve working with government partners, the private sector, and non-governmental and volunteer organizations to coordinate pre-disaster education and planning activities and lay the groundwork for coordinated disaster response.

### Response

Response is the actual provision of emergency services during a crisis including the coordination and management of resources to support emergency response operations. These activities help to reduce casualties and damage and to speed recovery. Response activities include alerting and notifying the public, resource, and logistical coordination, addressing immediate life safety issues, stabilization of the incident, and public information.

<<INSERT AGENCY ACRONYM HERE>> responds to emergencies by activating the Emergency Operations Plan, coordinating with public, private, and volunteer response partners as needed, coordinating, and managing resources in support of emergency response, and preparing for recovery activities.

### Recovery

Recovery activities may be both short-term and long-term, ranging from conducting damage assessments, removing debris, restoration of critical facilities/infrastructure, and essential utilities such as water and power, to providing assistance to member communities. Recovery may also incorporate mitigation measures designed to prevent future occurrences of a given hazard. Recovery begins as soon as possible after an incident occurs and may commence during the response phase.

# Organization and Assignment of Responsibilities

This section describes the organizational structure <<INSERT AGENCY ACRONYM HERE>> employs to respond to an emergency. It articulates the roles and responsibilities that various members of the emergency management organizational structure have in any response.

It includes:

* A list of the kinds of tasks to be performed by position and organization.
* An overview of who does what.

The director is not able to manage all the aspects associated with an incident without assistance. The director relies on other key personnel to perform tasks that will ensure the safety of employees during a crisis or critical incident. Each employee must be familiar with their role and responsibilities before an incident occurs.

## Organization

### Director

The director, or their designee, may serve as the Incident Commander until emergency responders arrive. At all times, the director retains the overall responsibility for the overall safety of employees. The director shall coordinate with first responders upon arrival.

### Administrative Staff

Responsibilities include:

* Survey and report building damage;
* Control main shutoff valves for gas, water, and electricity and ensure that no hazard results from broken or downed lines;
* Provide damage control as needed;
* Provide for the safety of essential records and documents; and
* Assist in the conservation, use, and disbursement of supplies and equipment.

### Supervisors

Responsibilities include:

* Supervise telecommunicators under their charge;
* Ensure telecommunicators are completing their assignments;
* Take steps to ensure the safety of employees in the implementation of incident management protocols;
* Direct employees to inside or outside assembly areas, in accordance with signals, warning, written notification, or orders according to established incident management procedures;
* Give appropriate action commands during an incident;
* Take attendance when relocated to an outside or inside rally point / assembly area or evacuates to another location;
* Report missing employees to the director;
* Execute assignments as directed; and
* Arrange for first aid for those unable to be moved and provide CPR, if needed.

### Telecommunicators

Responsibilities include:

* Answer phones and assist in receiving and providing consistent information to callers; and
* Perform work as directed by a supervisor or member of the administration.

# Direction, Control, and Coordination

## National Incident Management System

<<INSERT AGENCY ACRONYM HERE>>’s operation is structured in accordance with the National Incident Management (NIMS) and the Incident Command System (ICS). NIMS integrates existing processes and methods into a unified national framework for incident management. This framework forms the basis for interoperability and compatibility that enable a diverse set of public and private organizations to conduct effective incident management operations.

It does this through a core set of concepts, principles, procedures, organizational structures (Incident Command System, multi-agency coordination, and joint information systems), terminology, and standards requirements applicable to a broad community of NIMS users. To ensure interoperability and compatibility, NIMS is based on an appropriate balance of flexibility and standardization. It provides a consistent and flexible national framework within which government and private entities at all levels can work together to manage domestic incidents, regardless of their cause, size, location, or complexity.

## Incident Command System

Emergency management and incident response in <<INSERT AGENCY ACRONYM HERE>> is coordinated using the Incident Command System (ICS). ICS enables effective incident management by integrating a combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure. ICS is used to organize both near-term and long-term operations for a broad spectrum of emergencies, from small to complex incidents, both natural and manmade. ICS is used by all levels of government – federal, state, regional, and local – as well as by many private-sector and NGOs.

All activity undertaken under the EOP shall be coordinated using the Incident Command System (ICS) and the National Incident Management System (NIMS) in accordance with Homeland Security Presidential Directive (HSPD) 5.

### Incident Command

Single Incident Commander - Most incidents involve a single incident commander. In these incidents, a single person commands the incident response and is the decision-making authority.

### Unified Command

A Unified Command involves two or more individuals sharing the authority normally held by a single incident commander. Unified Command may be used during larger incidents, or incidents involving multiple agencies or jurisdictions. A Unified Command typically includes a command representative from major involved agencies and/or jurisdictions. A Unified Command acts as a single entity. It is important to note that in Unified Command the command representatives will appoint a single Operations Section Chief.

## Transfer of Command

Responsibility can be transferred during an incident for several reasons. As the incident grows a more qualified person may be required to take over as Incident Commander to handle the ever-growing needs of the incident. Or, this may occur in reverse; when an incident reduces in size, the command can be passed down to a less qualified person, but still qualified to run the now-smaller incident. Other reasons to transfer command include jurisdictional change if the incident moves to a different location or area of responsibility, or the normal turnover of personnel due to extended incidents. The transfer of command process always includes a transfer of command briefing, IC to IC, which may be oral, written, or a combination of both. A Transfer of Command is posted and announced on all radio and communication networks.

## Incident Coordination and/or Response Locations/Facilities

Various types of operational support facilities are established in the vicinity of an incident, depending on its size and complexity, to accomplish a variety of purposes. <<INSERT AGENCY ACRONYM HERE>> may operate one or more of the following incident coordination and/or response facilities, specifically for its employees, during an emergency or disaster:

* Incident Command Post
* Emergency Operations Center
* Staging Area
* Points of Distribution
* Evacuation Assembly Points
* Evacuation Transportation Hubs

### Incident Command Post

An Incident Command Post (ICP) is the field location where the Incident Commander operates, onsite response is directly coordinated, and onsite resource needs are identified and communicated. There is only one ICP for each incident or event, but it may change locations during the event. The ICP may be located in a vehicle, trailer, tent, or within a building. The ICP will be positioned outside of the incident scene and the potential hazard zone but close enough to the incident to maintain a visual presence and command status. The on-scene Incident Commander has tactical control of and authority over all resources at the scene.

## Line of Succession

There may be instances where an individual in a leadership position is unable or unavailable to carry out his or her duties. Orders of succession define who takes on these duties when an individual in a leadership position is unavailable or incapacitated in order to ensure there are no lapses in essential decision-making authority.

A successor will assume the duties of the leadership position in the following circumstances:

* The position is vacant due to the death, resignation, or removal of the incumbent.
* The incumbent is not physically present, cannot be contacted, and the situation requires that expeditious decisions are made, or actions are taken.

In all cases, the successor will have all the duties, powers, and responsibilities of the incumbent as they relate to the implementation of the COOP Plan. The successor will relinquish leadership duties when the incumbent is contacted and able to resume his or her leadership role, or when a permanent successor is named by the appropriate authority.

<<INSERT AGENCY ACRONYM HERE>> Center orders of succession are detailed in the COOP Plan on **page 2-27**.

# Information Collection, Analysis, and Dissemination

## Situational Awareness

During the initial period of an emergency, efforts should be focused on gaining an understanding of the situation and establishing incident priorities. A well-defined, operational information collection capability is essential. Information collection provides situational awareness to leadership and promotes informed decision-making. The center has designated a process to collect, analyze and disseminate information during an emergency to both internal and external response partners as well as the public.

## Information Collection

Information will be collected from a variety of sources. The Director or his/her designee at <<INSERT AGENCY ACRONYM HERE>> will be charged with collecting information. The following list contains examples of potential sources of operational information:

* <<DESCRIBE YOUR POTENTIAL SOURCES OF INFORMATION HERE>>

## Information Analysis

After the information has been collected, it must be analyzed to determine its credibility and operational relevance. The Director or his/her designee will analyze information that is received and prepare intelligence reports for leadership.

## Situation Reports (SitReps)

<<INSERT AGENCY ACRONYM HERE>> may issue Situational Reports (SitReps) from time to time to convey information as necessary to responders, community departments and agencies, and other partners. Additionally, when needed, <<INSERT AGENCY ACRONYM HERE>> will maintain and update an Incident Action Plan (IAP), which will contain critical information and intelligence updates. A copy of a SitRep template is available <<WHERE>> on SharePoint (see **page 8-1**).

Situation Reports should address the following areas:

* Date/Time
* Primary Topic Area
* Originator
* Next Advisory Date/Time
* <<INSERT AGENCY ACRONYM HERE>> Staffing Level
* Message Text
* Impact to <<INSERT AGENCY ACRONYM HERE>>
* Current Actions
* Future Actions/Needs
* Links of Interest
* Attachments

**Primary Topic Area**

The Primary Topic Area should indicate the main topic of the SitRep. Typically, this would be related to one of the hazards identified in the Threat, Hazard, and Vulnerability Analysis Summary Section of this document which can be found on **page 7**. However, given that not every possible emergency can be planned for, this field should address the most relevant topic.

**<<INSERT AGENCY ACRONYM HERE>> Staffing Level**

In this section, <<INSERT AGENCY ACRONYM HERE>> should detail its staffing level according to the agency’s COOP plan showing the operations level and the number of FTEs unable to work, as a percentage. For more information, refer to **page 2-1**.

**Message Text**

The Message Text field is where important situational alert messages should be placed.

**Impact on <<INSERT AGENCY ACRONYM HERE>> and/or Member Communities**

Any direct or planned impacts due to the emergency that are affecting <<INSERT AGENCY ACRONYM HERE>> and/or Member Communities should be added here.

**Current Actions**

In this section, <<INSERT AGENCY ACRONYM HERE>> and/or member communities’ current action(s) should be added. This may include changes to procedures, protocols, or other important actions that are being undertaken.

**Future Actions/Needs**

Message dissemination is categorized into has been crafted for public dissemination.

**Links of Interest**

Links of interest can be added in this section. This may include guidance from the National Weather Service, updates on the current emergency, or websites that may benefit member agencies during the emergency.

**Attachments**

Any attachments that are disseminated with the situation report should be listed in this section. Hardcopy dissemination of the SitRep shall include these attachments. Also, when possible, the soft copy of the SitRep should include all attachments.

## Public Messaging

Various methods of public information dissemination are available. The decision to use a particular medium will be based on the urgency and the intended audience. Some methods of distribution include:

* Press releases;
* Press conferences;
* Website updates;
* Print, radio, or televised announcements;
* Social media updates; and
* Emergency Notification Systems and/or web-based notification systems.

To ensure one consistent and accurate voice, all public information releases will be coordinated through Director or his/her designee.

# Communications

Communications are an important component of response and recovery operations. The ability of emergency personnel from different disciplines, jurisdictions, organizations, and agencies to work together depends greatly on their ability to communicate with each other. To effectively transmit and receive information, emergency response partners supporting the center and/or its member communities must have access to all available forms of communication. This section outlines the types of equipment/systems available for internal, external, and public communication that <<INSERT AGENCY ACRONYM HERE>> is able to access and/or provide. Operational communications systems and capabilities, and effective communications, are essential to the success of any emergency operation. <<INSERT AGENCY ACRONYM HERE>> maintains and operates the following communications systems to ensure effective and operational communications between municipal personnel and with other jurisdictions.

Communications between agencies occur through the use of several types of communications equipment including <<IDENTIFY YOUR COMMUNICATION METHODS HERE>>. Public communications range from the Emergency Alert System to <<INSERT AGENCY ACRONYM HERE>>’s website and social media.

<<INSERT AGENCY ACRONYM HERE>> maintains interdepartmental communication through the following:

* <<LIST INTERDEPARTMENTAL COMMUNICATION METHODS HERE>>.

## Alert and Notification

Emergency notification of community agencies is critical during times of emergency to ensure response partners have adequate time to prepare for an emergency and can assemble to respond to an emergency. The community has several means of notifying emergency response partners. In most situations, the Community has the capability to warn departments and agencies on a 24-hour basis.

## Notification of Key Officials

When an emergency requires the notification of key community officials, the <<INSERT AGENCY ACRONYM HERE>> will utilize the following means as appropriate:

* Email
* Landline telephone
* Cellular Phone
* Satellite Phone
* 2-way radio systems (during normal business hours)
* Dispatch a vehicle for in-person notification
* Face-to-face communication

## Public Information Officer

<<INSERT AGENCY ACRONYM HERE>> operates under the State 911 Department. The Director, or their designee, will work with the PIO to ensure important messages are disseminated.

The <<INSERT AGENCY ACRONYM HERE>> PIO is:

|  |
| --- |
| <<INSERT AGENCY PIO HERE>> |

Responsibilities of the PIO include:

* Determining or creating proper message content
* Select appropriate dissemination channel(s)
* Disseminate press releases and/or public warnings after receiving written approval Director

# Administration, Finance, and Logistics

## Finance and Administration

If existing <<INSERT AGENCY ACRONYM HERE>> resources and mutual aid resources are exhausted, or if <<INSERT AGENCY ACRONYM HERE>> has a need for a resource that it neither has nor has access to, <<INSERT AGENCY ACRONYM HERE>> should submit a request for assistance to <<IDENTIFY THE PROCESS OF REQUESTING OUTSIDE ASSISTANCE HERE>>.

## Recordkeeping

The <<WHO IS RESPONSIBLE FOR FINANCE>> is responsible for managing the expenditure of funds and providing reasonable accountability and justification for expenditures made to support incident management operations for the <<INSERT AGENCY ACRONYM HERE>>. These records may be used to recover costs from the responsible party or insurers or as a basis for requesting financial assistance for certain allowable response and recovery costs from the Federal government.

## Preservation of Records

In order to continue normal operations following an incident, vital records must be protected. The principal causes of damage to records are fire and water; therefore, essential records should be protected accordingly. A listing of essential records is detailed in the <<INSERT AGENCY ACRONYM HERE>> COOP Plan which can be found on **page 2-26**.

## Reports

The use of reports varies according to the type of emergency being handled.

### Messages

All requests for assistance and all general messages should be handled using the procedures and forms found in the Forms section of this plan.

Other forms may include the chronological log and daily staff journal log and financial tracking reports.

## Resource Management

The following are sources or potential sources for resources that may be available to <<INSERT AGENCY ACRONYM HERE>> in responding to disasters and emergencies:

* <<INSERT AVAILABLE RESOURCES, MUTUAL AID, ETC., HERE HERE>>

If existing <<INSERT AGENCY ACRONYM HERE>> resources and mutual aid resources are exhausted, or if <<INSERT AGENCY ACRONYM HERE>> has a need for a resource that it neither has nor has access to, <<INSERT AGENCY ACRONYM HERE>> should submit a request for assistance to <<IDENTIFY THE PROCESS OF REQUESTING OUTSIDE ASSISTANCE HERE>>.

The figure below depicts the process by which MEMA receives, processes, tracks, and fulfills requests from stakeholders for support.



## Mutual Aid

Mutual aid is the provision of services from one jurisdiction to another. A mutual aid agreement is an agreement among jurisdictions to allow emergency responders to lend assistance across [jurisdictional](https://en.wikipedia.org/wiki/Jurisdiction) [boundaries](https://en.wikipedia.org/wiki/Border). Some mutual aid agreements may be formal and/or may be activated with some degree of frequency, such as mutual aid provided in the fire services community. Other mutual aid agreements are informal, and/or activated infrequently and only under emergency circumstances.

<<INSERT AGENCY ACRONYM HERE>> has entered into the following mutual aid agreements:

* <<WHO IS YOUR ALTERNATE PSAP>> has entered into a Memorandum of Agreement to act as the Alternate PSAP for <<INSERT AGENCY ACRONYM HERE>>

# Training and Exercise Program

A critical component of this EOP is the ability to conduct training and exercises in order to validate the EOP’s contents. These events should take an all-hazards approach. In addition, training and exercises could focus on specific areas, such as hazardous materials events. A training and exercise program should be developed to effectively implement the EOP.

## Training Program

An all-hazards training program is a critical component of a community’s emergency planning cycle. The following sections describe some of the various training opportunities an Emergency Operations Plan can take advantage of.

### All-Hazards Training

**FEMA Independent Study Training**

FEMA has made numerous Independent Study (IS) courses available to first responders for free. All employees of the <<INSERT AGENCY ACRONYM HERE>> shall complete the following courses:

* IS-100.C: Introduction to the Incident Command System, ICS 100
* IS-200.C: Basic Incident Command System for Initial Response
* IS-700.B: An Introduction to the National Incident Management System
* IS-800.C: National Response Framework, an Introduction

**Emergency Management Institute Training**

The Emergency Management Institute (EMI) has a series of online Professional Development Training Programs designed to bolster the knowledge emergency managers need to possess. These online-based classes can be found on FEMA’s Emergency Management Institute Website, under their Professional Development Section.

**MEMA Provided Training**

MEMA’s Training and Exercise Unit offers numerous classroom training opportunities throughout the calendar year. These all-hazards training programs cover various topics and offer unique perspectives on emergency management planning and response. Specific training programs can be found on MEMA’s website.

Some examples of training include:

1. Incident Command Systems (ICS) 300;
2. Incident Command Systems (ICS) 400;
3. ICS for Elected and Senior Leaders;
4. Emergency Operations Center (EOC) Awareness and Operations; and
5. Homeland Security Exercise and Evaluation Program (HSEEP) Training.

**Incident Command System**

Incident Commanders, who will assume control of the incident scene or operate in a command post (including supervisory and administrative staff), shall receive the following training:

* ICS-300 Intermediate Incident Command System (Required)
* ICS-400 Advanced Incident Command System for Complex Incidents (Recommended)

Incident commanders shall also have competency in the following areas:

1. Know and be able to implement the employer’s incident command system.
2. Know how to implement the employer’s emergency response plan.
3. Know and understand the hazards and risks associated with employees working in chemical protective clothing.
4. Know how to implement the local emergency response plan.
5. Knowledge of the state Emergency Response Plan and of the Federal Regional Response Team.
6. Know and understand the importance of decontamination procedures.

## Exercise Program

Similar to Training Programs, this Emergency Operations Plan includes a training and exercise program to ensure that training and the various plans are effective.

Section 303(c)(9) of the Emergency Planning and Community Right-to-Know Act (EPCRA), places a requirement on local jurisdictions to establish “methods and schedules for exercising the emergency plan”. In establishing training programs and schedules the emergency managers recognize the need for an integrated exercise program that will ensure community response agencies and facilities successfully perform their emergency roles and functions in accordance with the All-Hazards Emergency Plan. An effective exercise program will also strengthen response management, coordination, and operations, plus reveal shortcomings and weaknesses that can be corrected prior to an emergency in order to improve and refine public safety capabilities.

### Types of Exercises

Exercises are generally classified into three major categories: Tabletop, Functional, and Full Scale. Local jurisdictions may also consider preliminary exercises called *Orientations* to introduce participants to the plan and prepare for the exercise process.

Each of these exercises varies in activities and resources. Some require simple preparations and execution while others may be more complex and require greater efforts and resources. Each provides its own benefits, and all should be considered in the overall development of an exercise program.

**Orientation (Exercise)**

*Orientations* are used to acquaint personnel with policies and procedures developed in the planning process, providing a general overview of the emergency plan and its provisions. Orientation is especially effective in ensuring that emergency personnel understand their roles and responsibilities and clarifying any complex or sensitive plan elements. While the orientation does not normally involve any direct simulation or role-playing, it is used to review plan procedures and informally apply them to potential emergency situations or past events familiar to everyone.

**Tabletop Exercise**

A *Tabletop Exercise* is primarily a learning exercise that takes place in a meeting room setting. Prepared situations and problems are combined with role-playing to generate discussion of the plan, its procedures, policies, and resources. *Tabletop Exercises* are an excellent method of familiarizing groups and organizations with their roles and demonstrating proper coordination. They are also good environments for reinforcing the logic and content of the plan and integrating new policies into the decision-making process since they allow participants to act out critical steps, recognize difficulties, and resolve problems in a non-threatening environment.

**Functional Exercise**

A *Functional Exercise* is an emergency simulation designed to provide training and evaluation of integrated emergency operations and management. It is more complex than the *Tabletop Exercise* and focuses on the interaction of decision making and agency coordination in a typical emergency management environment such as an Operating Center or command location. All field operations are simulated through messages and information normally exchanged using actual communications, including radios and telephones. It permits decision-makers, command officers, coordination, and operations personnel to practice emergency response management in a more realistic environment, complete with time constraints and stress. It generally includes several organizations and agencies practicing interaction of a series of emergency functions such as direction and control, assessment, and evacuation.

**Full-Scale Exercise**

The *Full-Scale Exercise* evaluates several components of an emergency response and management system simultaneously. It exercises the interactive elements of a community emergency program, similar to the *Functional Exercise*, but it is different from the *Functional Exercise* in that it adds a field component. A detailed scenario and simulation are used to approximate an emergency, which requires on-scene direction and operations, and also includes coordination and policy-making roles at an emergency operation or command center. Direction and control, mobilization of resources, communications, and other special functions are commonly exercised.

**Progressive Exercise Program**

Recognizing that the exercise types described in this plan are intended to build on one another, each one becoming more complex and comprehensive, the <<INSERT AGENCY ACRONYM HERE>> should establish a progressive exercise program by scheduling basic *Orientations* to introduce the plan and the specific policies and responsibilities established. *Tabletop Exercises* will then be held to implement actual coordination and leadership provisions of the plan, including emergency operations concepts that may be new to many personnel. These will be followed by *Functional Exercises* to integrate the plan’s more complex sections under simulated emergency conditions. Finally, a *Full-Scale* Exercise may be conducted to evaluate the overall plan.

**Exercise Schedule**

<<INSERT AGENCY ACRONYM HERE>> should create a multi-year Training and Exercise Program to test this EOP and annexes within it. At a minimum, at least one exercise should be held annually. However, if a real response situation has occurred, it may be counted as an exercise as long as an after-action evaluation is performed, and the plan is updated with “lessons learned” from the incident.

# Plan Development and Maintenance

If a plan is to be effective its contents must be known and understood by those who are responsible for its implementation. The Director shall brief the appropriate personnel concerning their roles and responsibilities under this Plan. The Director shall arrange for appropriate training and exercises to maintain this plan.

The Director, or their designee, is responsible for the administrative maintenance of this Plan and should ensure that this plan is reviewed and updated on an annual basis and that all appropriate personnel and departments participate in the review.

The Director is responsible for maintaining a training and exercise program that ensures that the Plan is exercised at least once each year. <<INSERT AGENCY ACRONYM HERE>> should annually review this Plan, update it as necessary, and incorporate any lessons learned/best practices identified through training, exercises, and actual events/incidents.

Following every exercise or significant real-world event, a designated <<INSERT AGENCY ACRONYM HERE>> employee will ensure that a detailed After-Action Report (AAR) and Improvement Plan is prepared.

# References

**1. Federal**

* The Federal Civil Defense Act of 1950 (PL 81-920)
* The Disaster Relief Act of 1974 (PL 93-288)
* Emergency Management and Assistance, 44 U.S. Code 2.1
* Homeland Security Presidential Directive (HSPD) 5, “Management of Domestic Incidents”
* Public Law-288
* National Response Plan (NRP)
* National Response Framework (NRF)
* CPG-101
* National Preparedness Goal
* National Incident Management System (NIMS)
* Incident Command System (ICS)

**2. Commonwealth of Massachusetts**

* Massachusetts Civil Defense Act, Chapter 33
* Massachusetts Executive Order 144
* Executive Order #242, Comprehensive All-hazards Emergency Planning
* Executive Order #469, Designation of the NIMS as the State’s Incident Management Standard
* Massachusetts EOC - Standard Operating Procedures
* State EOC Utilization Plan
* State Fire Mobilization Plan
* MEMA Continuity of Operations (COOP) Plan

**3. Industry Best-Practices**

**FEMA**

FEMA: [Federal Continuity Directive-1](https://www.fema.gov/media-library-data/1486472423990-f640b42b9073d78693795bb7da4a7af2/January2017FCD1.pdf) Federal Executive Branch National Continuity Program and Requirements, January 2017

FEMA: [Federal Continuity Directive-2](https://www.fema.gov/media-library-data/1499702987348-c8eb5e5746bfc5a7a3cb954039df7fc2/FCD-2June132017.pdf) Federal Executive Branch Mission Essential Functions and Candidate Mission Essential Functions Identification and Submission Process July 2017

**NFPA**

NFPA: [Standard 1600](https://www.nfpa.org/assets/files/AboutTheCodes/1600/1600-13-PDF.pdf): Standard on Continuity, Emergency, and Crisis Management

**NENA**

NENA has numerous policies, specific to PSAP Operations / Contingency Planning. More information is available at [www.nena.org](http://www.nena.org) under NENA standards & Other Documents.

NENA: NENA [Communications Center/PSAP Disaster and Contingency Plans](https://www.nena.org/resource/resmgr/standards/nena-inf-017.3-2018_disaster.pdf) Model Recommendation (53-001/NENA-INF-017.2.108)

NENA: [NENA PSAP Survivability Standard](https://www.nena.org/resource/resmgr/standards/NENA-INF-020.2-2017_PSAPSurv.pdf) (NENA-INF-020.2-2017)

1. Functional Annexes

The following sections contain the Functional Annexes of this EOP.

**Functional Annexes**

Functional annexes do not repeat content but rather build on the information within the basic plan. This includes all-hazard critical operational functions, including common or specialized procedures:

1. Annex – Continuity of Operations Plan

Continuity of Operations (COOP) Plan

Contents of COOP

[Purpose 2-4](#_Toc85625913)

[Applicability and Scope 2-4](#_Toc85625914)

[Planning Assumptions 2-5](#_Toc85625915)

[Core COOP Components 2-5](#_Toc85625916)

[Concept of Operations 2-9](#_Toc85625917)

[Phase I: Readiness and Preparedness 2-9](#_Toc85625918)

[Phase II: Activation 2-9](#_Toc85625919)

[Phase III: Operations 2-13](#_Toc85625920)

[Phase IV: Reconstitution 2-13](#_Toc85625921)

[COOP Responsibilities 2-14](#_Toc85625922)

[Agency/Organization Head 2-14](#_Toc85625923)

[Continuity Manager 2-14](#_Toc85625924)

[Emergency Relocation Group (ERG) Advance Team (A-Team) 2-14](#_Toc85625925)

[Designated ERG Personnel 2-15](#_Toc85625926)

[Alternate Facility Support Coordinator 2-15](#_Toc85625927)

[Reconstitution Coordinator 2-15](#_Toc85625928)

[Department/Division Management 2-16](#_Toc85625929)

[<<INSERT AGENCY ACRONYM HERE>> Center Staff 2-16](#_Toc85625930)

[Logistics 2-16](#_Toc85625931)

[Transition of Mission Essential Functions to Alternate Facility 2-16](#_Toc85625932)

[Return of Mission Essential Functions to the Primary Facility 2-17](#_Toc85625933)

[Interoperable Communications 2-17](#_Toc85625934)

[Procurement 2-18](#_Toc85625935)

[Testing, Training, and Exercises 2-18](#_Toc85625936)

[Testing 2-18](#_Toc85625937)

[Training 2-18](#_Toc85625938)

[Exercising 2-19](#_Toc85625939)

[After-Action Process 2-19](#_Toc85625940)

[COOP Plan Maintenance 2-19](#_Toc85625941)

[Authorities and References 2-21](#_Toc85625942)

[Appendix B: Emergency Relocation Group 2-23](#_Toc85625943)

[Appendix C: Mission Essential Functions 2-24](#_Toc85625944)

[Appendix D: Critical Systems 2-25](#_Toc85625945)

[Appendix E: Essential Records 2-26](#_Toc85625946)

[Appendix F: Orders of Succession and Delegations of Authority 2-27](#_Toc85625947)

[Appendix G.1: Contact List – Agency 2-28](#_Toc85625948)

[Appendix G.2: Contact List – Member Community 2-29](#_Toc85625949)

[Appendix H: Emergency Staffing Level Response Plan 2-30](#_Toc85625950)

[Appendix I: Business Impact Analysis Summary 2-31](#_Toc85625951)

[Appendix J: Definitions 2-33](#_Toc85625952)

[Appendix K: Acronyms 2-35](#_Toc85625953)

Purpose

The <<INSERT AGENCY ACRONYM HERE>> Center Continuity of Operations Plan (COOP) provides a framework to ensure continued operation of mission essential functions for up to 30 days when an internal or external emergency impacts the Agency’s facilities, systems, personnel, and/or operations. This COOP addresses all hazards, natural and manmade, and includes climate change considerations. The <<INSERT AGENCY ACRONYM HERE>> Center COOP establishes a concept of operations, strategies, and tactics to accomplish the following objectives:

* Ensure that <<INSERT AGENCY ACRONYM HERE>> can perform mission essential functions under all conditions.
* Successfully execute a timely and orderly recovery and reconstitution of mission essential functions by
  + Identifying key staff needed to continue mission essential functions.
  + Identifying and ensuring access to critical systems needed to support mission essential functions.
* Minimize disruptions to <<INSERT AGENCY ACRONYM HERE>>’s mission essential functions and operations.
* Ensure that <<INSERT AGENCY ACRONYM HERE>> has an alternate facility where it can carry out its mission essential functions in the event its primary facility is unusable or inaccessible.
* Execute a successful order of succession with accompanying designated authorities should an incident render key leadership unable or incapable of assuming and performing their authorities and/or responsibilities.
* Identify and protect essential records and other essential assets in the event of an incident, and ensure they are accessible at alternate facilities.
* Establish a training and exercise cycle to regularly test and validate the continuity of operations plans and procedures.

**Applicability and** **Scope**

The COOP applies to the staff and facilities of <<INSERT AGENCY ACRONYM HERE>> Center during any emergency incident that impacts the day-to-day operations of <<INSERT AGENCY ACRONYM HERE>>. The COOP must be implemented no later than 12 hours after activation of the Plan and provide guidance to sustain mission-essential operations for up to 30 days.

The Plan takes into account the full spectrum of threats, hazards, and emergencies that may disrupt <<INSERT AGENCY ACRONYM HERE>> Center’s normal day-to-day operations by rendering one or more of its facilities and/or systems inoperable or inaccessible and requiring <<INSERT AGENCY ACRONYM HERE>> Center to relocate staff and resources from impacted locations(s) to a designated Alternate Facility or to utilize backup or redundant systems. Such emergencies could include but are not limited to storms, utility or infrastructure failures, cyber incidents, terrorism incidents, or credible security threats. In addition, the COOP addresses circumstances that may incapacitate key staff members or significant numbers of staff for a significant period, such as during an infectious disease outbreak. Such circumstances may not require relocation of staff and resources but may require <<INSERT AGENCY ACRONYM HERE>> to reassign staff and/or implement orders of succession to ensure the continued operation of its mission essential functions.

Please note, the COOP is not an evacuation plan. While an emergency may require the evacuation of a facility with little or no advance notice, building evacuations are typically conducted in accordance with the Emergency Operations Plan for that location. In the event of an evacuation of a facility, the COOP provides guidance on the deliberate and preplanned movement of designated staff to an alternate facility once the evacuation of the facility is accomplished.

Planning Assumptions

* An incident or event affecting <<INSERT AGENCY ACRONYM HERE>> Center can occur at any time, with little or no warning, and have a severe impact on the agency, its facilities, systems or operations, and staff that may be called upon to continue agency operations.
* <<INSERT AGENCY ACRONYM HERE>> Center facilities may be rendered uninhabitable or unusable by an incident, requiring the use of an alternate facility.
* Mission Essential Functions must be continued, regardless of the magnitude of the impact of the incident affecting facilities, systems, or operations.
* In the event of a widespread or catastrophic disaster, staff may need to take steps to ensure their own safety and security, or that of their families, prior to reporting to work.
* Government agencies will take appropriate and timely action to ensure the continuance of essential program functions during an emergency or disaster.
* <<INSERT AGENCY ACRONYM HERE>> Center administration will exercise its authority to implement this COOP plan in a timely manner when confronted with real or threatened disasters.
* The Commonwealth is committed to supporting service resumption and recovery efforts at continuity facilities if required.
* If properly implemented, this plan will reduce or prevent disaster-related losses.

Core COOP Components

There are several core components of continuity planning:

* Defining mission essential functions;
* Identifying critical staff to carry out mission essential functions;
* Identifying interdependencies critical to mission essential functions;
* Identifying critical systems required for mission-essential functions;
* Designating alternate facilities where mission essential functions can be implemented;
* Identifying appropriate and lawful orders of succession;
* Defining delegations of authority;
* Identifying essential records that are required to support mission essential functions or are required to by law to be maintained; and
* Ensuring resources, such as fly-away kits, are maintained and available to support COOP activation.

Each core COOP component is described in detail in the following sections.

1. **MISSION ESSENTIAL FUNCTIONS**

Mission Essential functions are defined as those functions of <<INSERT AGENCY ACRONYM HERE>> Center required to accomplish core components of <<INSERT AGENCY ACRONYM HERE>> Center’s mission as defined by applicable laws, executive orders, and/or other policies or directives. These functions cannot be halted due to any circumstance and are critical to the Agency’s operation. As part of the development process of the COOP Plan, <<INSERT AGENCY ACRONYM HERE>> Center has conducted a Business Impact Analysis (BIA) in order to identify and prioritize its mission essential functions. A summary of BIA findings may be found on **page 2-31** of this plan.

**Page 2-24** of this plan contains a prioritized list of <<INSERT AGENCY ACRONYM HERE>> Center’s mission essential functions.

1. **CRITICAL STAFF**

The COOP identifies and designates roles and responsibilities for continuity activations and operations, as well as minimum staffing requirements for activation of each mission-essential function. Critical staff includes:

* **Director and designee(s).** The Director and/or designee(s) is ultimately responsible for ensuring that <<INSERT AGENCY ACRONYM HERE>> Center is able to continue to perform mission essential functions and deliver critical services when normal operations are disrupted. The Director and/or designees have the authority to activate the continuity plan. Other members of the senior leadership may advise the Director and/or designee(s) on whether to activate the COOP.
* **Continuity Manager.** The Continuity Manager is responsible for coordinating overall continuity activities within <<INSERT AGENCY ACRONYM HERE>>, including managing day-to-day continuity programs, coordinating efforts of continuity planners, representing the continuity program externally as appropriate, and reporting to the Director on continuity program activities.
* **Emergency Relocation Group**. In the event of a continuity plan activation, the Emergency Relocation Group (ERG) is comprised of staff assigned to perform mission essential functions and deliver critical services until such time as additional plans are developed and implemented by the agency.
* **Emergency Relocation Group Advance Team.** The Emergency Relocation Group Advance Team is comprised of ERG staff who immediately deploy to the Alternate Facility upon being notified of COOP activation to stand up the Alternate Facility and ready it for all ERG personnel.
* **Reconstitution Coordinator.** The Reconstitution Coordinator is responsible for planning and managing the <<INSERT AGENCY ACRONYM HERE>>’s transition back to normal operations, including facilities, personnel, and systems.
* **Alternate Facility Support Coordinator.** The Alternate Facility Support Coordinator is the chief point of contact for the <<INSERT AGENCY ACRONYM HERE>> Center Alternate Facility and will work with the Continuity Manager and the ERG Advance Team to establish and maintain <<INSERT AGENCY ACRONYM HERE>> Center operations at the Alternate Facility.
* **All Employees.** Because a continuity plan activation impacts the entire organization, all employees are responsible for understanding their roles and responsibilities when the continuity plan is activated. Personnel who are not identified as part of the ERG may be required to replace or augment pre-designated ERG personnel during the implementation of the COOP Plan. This will be coordinated between the Continuity Manager and direct supervisors/managers on a case-by-case basis.

**Page 2-23** lists the current <<INSERT AGENCY ACRONYM HERE>> Center Critical COOP staff.

1. **INTERDEPENDENCIES**

Some agency mission essential functions may be dependent upon external systems, organizations, or supports. These systems, organizations, and supports are known as interdependencies, and those associated with <<INSERT AGENCY ACRONYM HERE>> Center’s mission essential functions have been identified as part of the BIA process and can be found on **page 2-24**.

1. **CRITICAL SYSTEMS**

The COOP identifies various tasks, functions, and systems that are important to the continuation of mission essential functions. This includes, but is not limited to, communications and information systems, and may include other specialized equipment and systems. A list of mission-critical systems is included on **page 2-25**.

1. **ALTERNATE FACILITIES**

Alternate Facilities are locations to which ERG staff can report and implement mission essential functions. Alternate Facilities must be capable of supporting operations in a threat-free environment in the event that mission essential functions and supporting staff are relocated to the site. An Alternate Facility must have sufficient space and equipment to sustain operations for a period of up to 30 days. It should also have available the telecommunication and information systems, records, and databases required to support the implementation of mission essential functions.

<<INSERT AGENCY ACRONYM HERE>> Center Alternate Facilities are detailed on **page 2-22**.

1. **ORDERS OF SUCCESSION**

There may be instances where an individual in a leadership position is unable or unavailable to carry out his or her duties. Orders of succession define who takes on these duties when an individual in a leadership position is unavailable or incapacitated in order to ensure there are no lapses in essential decision-making authority.

A successor will assume the duties of the leadership position in the following circumstances:

* The position is vacant due to the death, resignation, or removal of the incumbent.
* The incumbent is not physically present, cannot be contacted, and the situation requires that expeditious decisions are made, or actions are taken.

In all cases, the successor will have all the duties, powers, and responsibilities of the incumbent as they relate to the implementation of the COOP Plan. The successor will relinquish leadership duties when the incumbent is contacted and able to resume his or her leadership role, or when a permanent successor is named by the appropriate authority.

<<INSERT AGENCY ACRONYM HERE>> Center orders of succession are detailed on **page 2-27**.

1. **DELEGATIONS OF AUTHORITY**

This COOP identifies delegations of authority to ensure appropriate individuals are authorized to act on behalf of the organization head or other officials for specified purposes and to carry out specific duties. Delegations of authority will generally specify a particular function that an individual is authorized to perform and includes restrictions and limitations associated with that authority.

<<INSERT AGENCY ACRONYM HERE>> Center delegations of authority are detailed on **page 2-27**.

1. **ESSENTIAL RECORDS**

Essential records are documents, references, and records, regardless of media type, that are needed to support mission essential functions under the full spectrum of emergencies and disasters. Such records include those documents needed to meet operational responsibilities under emergency conditions (emergency operating records) or to protect the legal and financial rights of the government and those affected by government activities (legal and financial rights records).

Examples of essential records include:

* Standard operating procedures;
* Continuity plan and other emergency operations plans;
* Personnel and payroll records;
* Contracts;
* Vendor agreements;
* Memoranda of agreement and understanding;
* Orders of succession; and
* Delegations of authority.

Essential records must be protected from damage or destruction. In addition, the <<INSERT AGENCY ACRONYM HERE>> Continuity Manager must ensure that databases and other essential records needed to support the mission essential functions of the Agency are prepositioned at each Alternate Facility, carried with deploying personnel, and/or available through redundant or backup processes.

<<INSERT AGENCY ACRONYM HERE>> Center's essential records are detailed on **page 2-26**.

1. **COOP GO-KITS**

Go-Kits are containers that are readily available and easily transportable that include copies of standard operating procedures, emergency plans, contact lists, key documents, and other information or guidance that is not already pre-positioned at or accessible from the Alternate Facility.

Concept of Operations

0T0TThere are four phases of continuity operations: (1) readiness and preparedness, (2) activation, (3) operations, and (4) reconstitution. These four phases are used to build continuity processes and procedures, establish goals and objectives, and support the performance of organizational mission essential functions during an emergency.

Phase I: Readiness and Preparedness

Readiness and preparedness are measured by the ability of an organization to respond to a continuity activation. Readiness and preparedness activities include the following:

* Regularly review the COOP plan to ensure all COOP components are up-to-date and accurate;
* Designate COOP personnel;
* Monitor staffing levels using Appendix H and adjust operational services, as required;
* Identify and prepare an Alternate Facility, ensuring that it remains accessible and ready for activation, and critical systems and essential records are maintained;
* Ensure COOP Go-Kits are kept up-to-date;
* Secure important papers/documents daily;
* Save electronic documents on network drives rather than computer hard drives;
* Create off-site backups of critical files;
* Test backup and restoration processes of critical systems;
* Train on COOP responsibilities for COOP staff;
* Cross-train staff on various COOP positions;
* Encourage staff to develop family emergency plans to ensure the well-being of loved ones during an incident; and
* Exercise the COOP plan.

Phase II: Activation

The activation phase includes the decision-making process for activating the COOP, notification to and activation of COOP personnel, relocation to an alternate facility, initiation of mission essential functions, and transition of essential records and databases, and equipment involved with these functions.

1. Decision Process

Authorized individuals must decide whether to activate the COOP when conditions may threaten or impede the ability of the agency to carry out mission essential functions. These conditions may include:

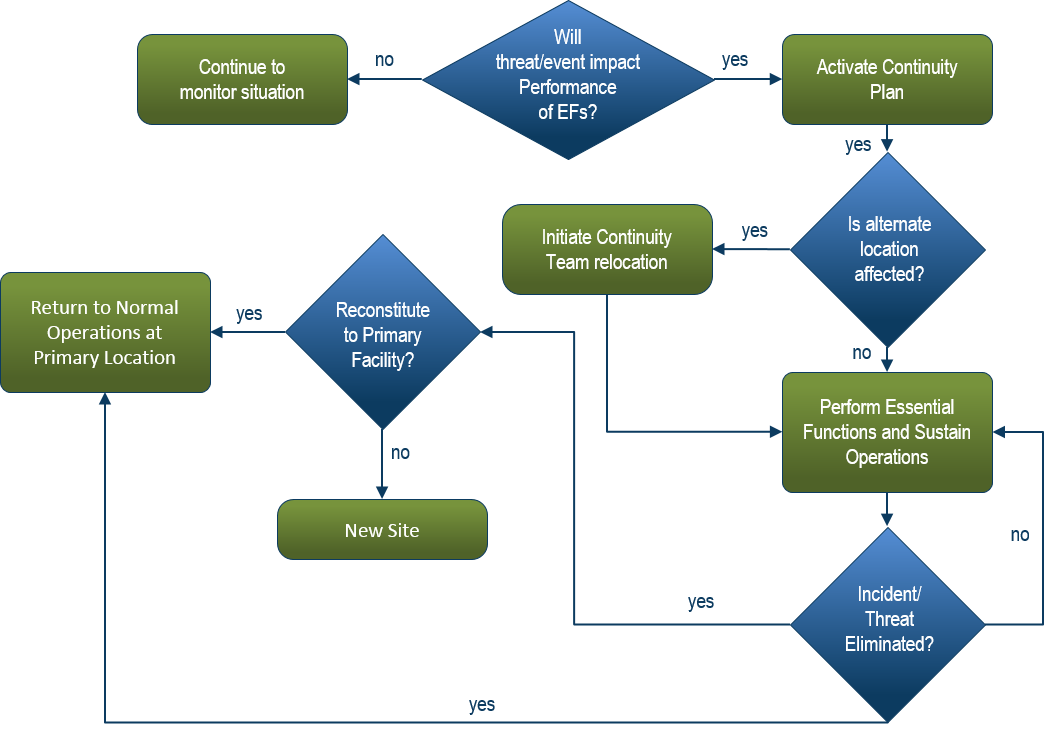
* Notification of a credible threat, which leads the organization to enhance its readiness posture and prepare to take necessary actions;
* An emergency or a disruption to personnel, facilities, equipment, or other necessary resources necessary to perform mission essential functions
* Evacuation of a geographical area

The Director or designee will 0T0Tconvene a team of senior leadership and/or staff, including the Continuity Manager, to review the situation and determine if the continuity plan should be activated.

0T0TThe Director will make the final decision to activate the COOP plan, taking into account the following factors:

* 0T0TDirection or guidance from higher authorities
* 0T0THealth and safety of <<INSERT AGENCY ACRONYM HERE>> Center personnel
* 0T0TAbility to carry out mission essential functions at the primary operating facility
* 0T0TChanges in threat advisories
* 0T0TIntelligence reports
* 0T0TPotential or actual effects on communications systems, information systems, office facilities, and other vital equipment.
* 0T0TAnticipated duration of the emergency situation

0T0T**Example Decision-Making Flowchart:**



Whenever feasible, the operation of mission essential functions will continue at the primary operating facility until they can be activated at the alternate facility.

1. Notification

When a decision to activate the COOP is made, all staff will be notified, according to the table below.

|  |  |  |
| --- | --- | --- |
| **Staff Type** | **Notification Method** | **Notification Message** |
| **Emergency Relocation Group (ERG) Advance Team** | Paging, Text, Email, Cellular Telephone | COOP Plan has been activated. Immediately proceed to and begin preparing the identified Alternate Facility. \*If applicable, provide information on routes or other appropriate safety precautions. \* **See page 2-22 for a list of Alternate Facilities** |
| **Emergency Relocation Group (ERG)** | Paging, Text, Email, Cellular Telephone | COOP Plan has been activated. When notified by the ERG Advance Team, proceed to the identified Alternate Facility. \*If applicable, provide information on routes or other appropriate safety precautions. \* **See page 2-22 for a list of Alternate Facilities** |
| **All Other Staff** | Paging, Text, Email, Cellular Telephone | COOP Plan has been activated. All non-COOP staff should report to the alternate facility/go home/implement telecommuting. If applicable, provide information on routes or other appropriate safety precautions. |

<<INSERT AGENCY ACRONYM HERE>> Center contact lists are detailed beginning on **page 2-28**.

1. Relocation and Activation of Mission Essential Functions

Upon notification, the following staff will implement their respective responsibilities.

**Continuity Manager:**

* The Continuity Manager notifies the Alternate Facility Support Coordinator that the ERG is enroute to the Alternate Facility.
* The Continuity Manager notifies other Agency offices outside the affected area and clients/stakeholders, as appropriate, that the activation of the COOP Plan is in progress.
* Notify vendors and service providers that <<INSERT AGENCY ACRONYM HERE>> Center has implemented its COOP Plan and provide direction on continuing or suspending services.

**Emergency Relocation Group Advance Team:**

* Upon notification, members of the Emergency Relocation Group (ERG) Advance Team will immediately travel to the appropriate Alternate Facility with fly-away kits.
* Upon arrival at the Alternate Facility, the Advance Team will ready the facility for implementation of mission essential functions
* When the Alternate Facility is ready, the Advance Team will notify the remaining members of the ERG.

**Emergency Relocation Group:**

* Upon notification from the Advance Team, the remaining members of the ERG will travel to the appropriate Alternate Facility.
* Upon arrival at Alternate Facility, activate mission essential functions.

**All Other Staff**

* All other staff will proceed as instructed in their COOP activation notification.

1. Transition of Responsibilities to the Deployed ERG:

* If operations of mission essential functions were able to be continued at the primary operating facility until the alternate facility is activated, the Director, or designee, will cease mission-essential function operations at primary operation location(s) when the Continuity Manager notifies the Director that mission essential functions are ready to be activated at the alternate facility.
* The Continuity Manager notifies other offices outside the affected area, external stakeholders, and other partners that Agency operations have shifted to the Alternate Facility.
* As appropriate, the Continuity Manager, or designated representative, notifies vendors and other service providers that Agency operations have been relocated temporarily and provides direction to either continue or temporarily suspend the provision of service.

Phase III: Operations

The operations phase covers the implementation and execution of the strategies identified in the continuity plan to ensure that the mission essential functions are accomplished. The operations phase includes, but is not limited to:

* Performing mission essential functions;
* Accounting for personnel, including identifying available leadership;
* Establishing communications with interdependent organizations and other internal and external stakeholders, including the media and the public;
* Providing guidance to all personnel; and
* Preparing for the recovery of the organization.

Phase IV: Reconstitution

0T0TReconstitution is the process by which the Agency returns to normal operations. Following a period of limited operations due to a threat, hazard, or emergency, reconstitution can be as simple as communicating to stakeholders that offices and facilities will re-open and commence normal operations and that all employees are expected to report to work for normal operations. Reconstitution can also be as complicated as recovering from complete destruction of a facility with challenges that include relocating operations, conducting mission essential functions with survivors, and identifying and outfitting a new permanent operating facility.

Reconstitution efforts generally begin when the Director, or another authorized person, ascertains that the emergency situation has ended and is unlikely to reoccur. However, once the appropriate <<INSERT AGENCY ACRONYM HERE>> official determines that the emergency has ended, immediate reconstitution may not be practical. Depending on the situation, one of the following options should be considered for implementation:

* Continue to operate from the Alternate Facility
* Return to the primary operating facility
* Transition to another longer-term facility

Prior to relocating to the primary operating facility or another long-term facility, <<INSERT AGENCY ACRONYM HERE>> will conduct appropriate security, safety, and health assessments to determine building suitability. In addition, the Reconstitution Coordinator will verify that all systems, communications, and other required capabilities are available and operational and that <<INSERT AGENCY ACRONYM HERE>> is fully capable of accomplishing all mission essential functions and operations at the new or restored facility.

* <<INSERT AGENCY ACRONYM HERE>> will notify all personnel by telephone and email using existing procedures and emergency notification tools that the emergency or threat of emergency has passed.
* If the primary operating facility will be uninhabitable or unusable permanently or for an extended period of time, the <<INSERT AGENCY ACRONYM HERE>> Director and the Reconstitution Coordinator will coordinate with the Division of Capital Asset Management and Maintenance to obtain appropriate office space for reconstitution.

Upon verification that all required capabilities are available and operational and that <<INSERT AGENCY ACRONYM HERE>> is fully capable of accomplishing all mission essential functions and operations at the new or restored facility, the Continuity Manager, in coordination with the Reconstitution Coordinator, will transition mission essential functions from the Alternate Facility to the new or restored primary operating facility.

COOP Responsibilities

Agency/Organization Head

* Provides overall policy direction, guidance, and objectives for continuity planning.
* Provides necessary resources to support the implementation of the <<INSERT AGENCY ACRONYM HERE>> COOP Plan and supporting activities.
* Ensures adequate funding is available for emergency operations.
* Ensures all <<INSERT AGENCY ACRONYM HERE>> Center components participate in testing, training, and exercise activities.

Continuity Manager

* Serves as the <<INSERT AGENCY ACRONYM HERE>> Center COOP program point of contact.
* Coordinates implementation of the COOP Plan and initiates appropriate notifications inside and outside <<INSERT AGENCY ACRONYM HERE>> during COOP Plan implementation.
* Coordinates the COOP Training, Testing, and Exercising Program.
* Aids ERG efforts at the Alternate Facility.
* Initiates recovery of <<INSERT AGENCY ACRONYM HERE>>, as part of reconstitution and designates a Reconstitution Coordinator.
* Maintains current personnel emergency notification and relocation rosters.
* Prepares backup copies or updates of essential records.
* Ensures that the time and attendance function is represented on the ERG.
* Designates personnel to assist security officials in securing office equipment and files at <<INSERT AGENCY ACRONYM HERE>> locations when implementing the COOP Plan.
* Conducts periodic tests of <<INSERT AGENCY ACRONYM HERE>> COOP notification methods and systems.

Emergency Relocation Group (ERG) Advance Team (A-Team)

* A subset of the larger ERG, who deploys to the Alternate Facility in advance of the ERG to prepare it for ERG arrival
* Ensures that COOP Go-Kits are maintained and ready for deployment.
* Works with Alternate Facility Support Coordinator and assigned staff to ready the Alternate Facility
* Ensures infrastructure systems at the alternate facility are fully operational, including power, HVAC, and communications systems such as telephone, internet, and radio.
* Ensures sufficient parking, equipment, materials, and supplies are present at the alternate facility to support the restoration of Mission Essential Functions.
* Once the Alternate Facility is ready, work with other ERG members to integrate into the facility to begin to execute Mission Essential Functions.
* Continues to work with the Alternate Facility Support Coordinator to address any issues as the relocation is ongoing and supports the reconstitution efforts once the decision is made to do so.

Designated ERG Personnel

* Be prepared to deploy and support mission essential functions in the event of COOP Plan implementation.
* Ensure managers/supervisors have up-to-date contact information.
* Be familiar with continuity planning and their individual roles and responsibilities in the event of COOP Plan implementation.
* Maintain COOP Go-Kits kits as needed.
* Participate in continuity training and exercises as directed.

Alternate Facility Support Coordinator

* Prepares site support plans to facilitate the smooth transition of direction and operations from <<INSERT AGENCY ACRONYM HERE>>’s primary location(s) to the Alternate Facility.
* Provides for the proper storage of backup copies of essential records and other pre-positioned items.
* Designates personnel responsible for assisting the arriving ERG Advance Team.
* Maintains a current roster of designated site support staff.
* Supports periodic coordination visits by <<INSERT AGENCY ACRONYM HERE>> officials.
* Keeps the Continuity Manager informed of site vulnerabilities or changes in site resources that may impact the effective implementation of the COOP Plan.
* Conducts an annual security risk assessment of the Alternate Facility by security staff to assist in ensuring COOP relocation site readiness.
* Facilitates periodic coordination visits by the Continuity Manager and other critical COOP staff to the Alternate Facility.
* Participates in scheduled tests, training, and exercises as appropriate.

Reconstitution Coordinator

* Assesses the status of affected facilities (as applicable) and determines how much time is needed to repair the affected facilities and/or the necessity of acquiring new facilities
* Supervises facility repairs, if the decision is made to return to the primary operating facility;
* If <<INSERT AGENCY ACRONYM HERE>> will not be able to return to the primary operating facility permanently or for an extended period of time, work with Director and DCAMM to obtain appropriate office space for reconstitution.
* Assesses the status of personnel post-incident to determine their availability to return to work
* Informs all personnel that the actual emergency, or the threat of an emergency, and the necessity for continuity operations no longer exists, and instructs personnel on how to resume normal operations;
* Verifies that all systems, communications, and other required capabilities are available and operational at the new or restored primary operating facility and that the organization is fully capable of performing all functions, not just essential ones, at the new or restored primary operating facility;
* Implements a priority-based phased approach to reconstitution by continuing mission essential functions at the alternate operating facility while non-essential functions return to the new or restored primary operating facilities as the organization conducts a smooth transition from one location to the other; and
* Supervises the return of operations, personnel, records, and equipment to the primary or other operating facilities.

Department/Division Management

* Appoints a point of contact for coordination and implementation of the COOP Plan.
* Keeps the Continuity Manager informed of any changes in the designation of the Department/Division COOP point of contact.
* Identifies mission essential functions to be performed by the Department/Division when any element of <<INSERT AGENCY ACRONYM HERE>> is relocated as part of the continuity planning process.
* Identifies those functions that can be deferred or temporarily terminated in the event the COOP Plan is implemented.
* Maintains a current roster of Department/Division personnel designated as ERG members.
* Maintains accountability of staff in the event that the COOP Plan is implemented.

<<INSERT AGENCY ACRONYM HERE>> Center Staff

* Review and understand the procedures in the Occupant Emergency Plan for emergency evacuation of <<INSERT AGENCY ACRONYM HERE>> Center facilities.
* Review and understand responsibilities related to COOP support functions and performance of <<INSERT AGENCY ACRONYM HERE>> Center mission essential functions at the Alternate Facility.
* Report to work to perform mission essential functions as detailed in this COOP plan or as requested.
* Ensure managers/supervisors have up-to-date contact information.

Logistics

Transition of Mission Essential Functions to Alternate Facility

Upon notification of COOP implementation, ERG advance team members will deploy to the designated Alternate Facility from their current location at the time specified during notification (which may be immediate). After arriving at the Alternate Facility, advance team members will, in conjunction with the Alternate Facility Support Coordinator, ready the facility for implementation of mission essential functions by:

* Ensuring infrastructure systems at the alternate facility are fully operational, including power, HVAC, and communications systems such as telephone, Internet, and radio.
* Ensuring sufficient equipment, materials, and supplies are present at the alternate facility to support the restoration of mission essential functions.
* Notifying vendors and service providers that <<INSERT AGENCY ACRONYM HERE>> operations have been relocated temporarily and provide direction to continue or suspend the provision of services.

When the Alternate Facility is ready, the Advance Team will notify the remaining members of the ERG. Upon arrival at the Alternate Facility, ERG personnel will:

* Report to the advance team lead and receive all applicable instructions and equipment
* Report to their respective workspaces as notified during the check-in process
* Retrieve any pre-positioned information and activate specialized systems or equipment
* Monitor the status of department personnel and resources
* Restore and continue departmental mission essential functions
* Coordinate with the ERG Advance Team or Continuity Manager to resolve issues.

Return of Mission Essential Functions to the Primary Facility

The Reconstitution Coordinator, with the assistance of <<INSERT AGENCY ACRONYM HERE>> facilities and IT staff, will assess the ability of the primary facility to resume supporting mission essential functions, ensuring that all systems and capabilities are fully operational, including:

* HVAC
* Sanitation
* Radio and telephone communications
* Internet access and access to data on shared Agency network drives

Once the primary facility is capable of supporting mission essential functions and with the concurrence of the <<INSERT AGENCY ACRONYM HERE>> Director and Continuity Manager, the Reconstitution Coordinator will supervise the return of operations, personnel, records, and equipment to the facility.

Interoperable Communications

The success of <<INSERT AGENCY ACRONYM HERE>> operations at the Alternate Facility depends upon the availability and redundancy of significant communication systems to support connectivity to internal organizations, other agencies, critical customers, and the public. Interoperable communications should provide a capability to correspond with the <<INSERT AGENCY ACRONYM HERE>>’s mission essential functions, to communicate with other Federal agencies, State agencies, and emergency support personnel, and to access other data and systems necessary to conduct all activities.

Procurement

<<INSERT AGENCY ACRONYM HERE>> may need to procure or augment necessary personnel, equipment, and supplies that are not already in place for continuity operations on an emergency basis. The Continuity Manager will coordinate with appropriate personnel to conduct any emergency procurement or hiring activities.

Testing, Training, and Exercises

Testing

Testing demonstrates the correct operation of all equipment, procedures, processes, and systems that support <<INSERT AGENCY ACRONYM HERE>>’s continuity program and ensures that resources and procedures are kept in a constant state of readiness. <<INSERT AGENCY ACRONYM HERE>> will test the following:

* Alert and notification systems and procedures for all employees and continuity personnel
* Protection, access, and recovery strategies found in continuity and disaster recovery plans for essential records, critical information systems, services, and data
* Internal and external interoperability and functionality of primary and backup communications systems
* Backup infrastructure systems and services, such as power, water, and fuel
* Other systems and procedures necessary to the organization’s continuity strategy, such as the IT infrastructure required to support telework options during a continuity plan activation
* Measures to ensure accessibility for employees and members of the public with access and functional needs

Training

Training familiarizes individuals with roles, responsibilities, plans, and procedures for conducting mission essential functions and providing critical services when normal operations are disrupted. On a continuous basis, 0T0T<<INSERT AGENCY ACRONYM HERE>> will train staff on:

* Expectations, roles, and responsibilities during a continuity plan activation and how these aspects differ from normal operations for all personnel
* Continuity plans and strategies, such as relocation, mutual aid agreements, and telework, for those identified to perform mission essential functions and provide critical services during a continuity plan activation
* Backup communications and IT systems that may be necessary to support or sustain mission essential functions for those expected to use such systems
* Orders of succession and delegations of authority for those individuals filling positions outlined within those documents

Exercising

Exercises play a vital role in preparedness by enabling partners, stakeholders, and elected officials to shape planning, test and validate plans and capabilities, and identify and address gaps and areas for improvement. <<INSERT AGENCY ACRONYM HERE>> will exercise the following at least once yearly as part of its overall continuity of operations program:

* Continuity plans and procedures in order to validate the organization’s strategy and ability to continue its mission essential functions and services
* Intra- and interagency backup communications capabilities
* Backup data and records systems required to support mission essential functions for sufficiency, completeness, currency, and accessibility
* Internal and external interdependencies, including support to mission essential functions and services and situational awareness
* Recovery from the continuity plan activation and environment and transition back to normal operations

After-Action Process

After activating or exercising the COOP Plan, the Continuity Manager will conduct an After-Action Review (AAR) with all department/division heads and ERG personnel as soon as possible following the return to the primary operating facility or establishment in a new primary operating facility. This review will study the effectiveness of COOP plans and procedures, identify best practices and areas of improvement, and document these in an After-Action Report and Improvement Plan.

COOP Plan Maintenance

To maintain viable COOP capabilities, <<INSERT AGENCY ACRONYM HERE>> is continually engaged in a process to designate mission essential functions and resources, define short- and long-term COOP goals and objectives, forecast budgetary requirements, anticipate and address issues and potential obstacles, and establish planning milestones. Following is a list of standardized activities necessary to monitor the dynamic elements of the <<INSERT AGENCY ACRONYM HERE>> COOP Plan and the frequency of their occurrence.

| **Activity** | **Tasks** | **Frequency** |
| --- | --- | --- |
| Plan update and certification | * Ensure COOP considers current hazards and risks, including natural and manmade hazards, and climate change considerations * Review the entire plan for accuracy. * Incorporate lessons learned and changes in policy and philosophy. * Manage distribution. | Annually |
| Maintain orders of succession and delegations of authority | * Identify the current incumbents. * Update rosters and contact information. | Semiannually |
| Maintain emergency relocation site readiness | * Check all systems. * Verify accessibility. * Cycle supplies and equipment as necessary. | Monthly |
| Monitor and maintain essential records management program | * Monitor the volume of materials. * Update/remove files. | Ongoing |

Authorities and References

Authority, support, and justification for continuity of operations (COOP) planning are provided through the documents listed below.

**Federal Guidance**

***Federal Continuity Directives (FCDs) 1 and 2.*** These are directive documents intended for federal executive branch departments and agencies. They provide operational direction for developing continuity plans and programs and are intended to achieve seamless integration by providing common standards and parameters to all continuity partners.

**FEMA Continuity Guidance Circular (CGC) 1**. This is a resource for federal and non-federal entities to guide, update, and maintain organizational continuity planning efforts and appropriately integrate and synchronize continuity efforts.

Commonwealth of Massachusetts Guidance

***Governor’s Executive Order No. 144.*** EO 144 requires all Commonwealth Agencies to prepare for emergencies and disasters and to provide emergency liaisons to the Massachusetts Emergency Management Agency/Organization for coordinating resources, training, and operations.

***Commonwealth of Massachusetts Chapter 639 of the Acts of 1950, Chapter 33*.**  The legislation provides basic Civil Defense / Emergency Management responsibilities for meeting dangers presented to the Commonwealth and its people by emergencies and disasters. The document directs preparedness efforts related to the common defense, protection of public peace, health, security, and safety.

<<INSERT AGENCY ACRONYM HERE>> Center Guidance

* <<IDENTIFY ANY APPLICABLE POLICIES/PROCEDURES THAT YOUR AGENCY HAS HERE>> Appendix A: Alternate Facility Information

<<INSERT AGENCY ACRONYM HERE>> has designated the following location to serve as an Alternate Facility for the Regional Emergency Communications Center

| **Emergency Relocation Site Information** | |
| --- | --- |
| Facility Name | <<IDENTIFY YOUR ALTERNATE SITE HERE>> |
| Address | <<IDENTIFY YOUR ALTERNATE SITE HERE>> |
| Phone Number | <<IDENTIFY YOUR ALTERNATE SITE HERE>> |
| Alternate Facility Point of Contact | <<IDENTIFY YOUR ALTERNATE SITE HERE>> |
| Directions | <<IDENTIFY YOUR ALTERNATE SITE HERE>> |
| Map | <<IDENTIFY YOUR ALTERNATE SITE HERE>> |

Appendix B: Emergency Relocation Group

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Functional Title | Name | Work Location | Email | 24-Hour Contact | Advance Team? (Y/N) |
| Manager | \* | \* | See page 2-28 | See page 2-28 | Y |
| Supervisor | \* | \* | See page 2-28 | See page 2-28 | Y |
| Supervisor | \* | \* | See page 2-28 | See page 2-28 | Y |
| Telecommunicator | \* | \* | See page 2-28 | See page 2-28 | Y |
| Telecommunicator | \* | \* | See page 2-28 | See page 2-28 | Y |
| IT | \* | \* | See page 2-28 | See page 2-28 | Y |
| Radio | \* | \* | See page 2-28 | See page 2-28 | Y |

\*The name and work location will be determined for each incident, dependent on staffing levels available, and relocation of which center, or both, therefore, name and location are intentionally blank on this form.

Appendix C: Mission Essential Functions

## 

| **Mission Essential Function** | **Recovery Time Objective** | **Responsible Personnel** | |
| --- | --- | --- | --- |
| <<IDENTIFY MEF HERE>> | 20 min | <<INSERT AGENCY ACRONYM HERE>> Director | |
| **Resources** | |  |
| <<IDENTIFY HERE>> | |  |
| **Work Location & Space Requirements** | |  |
| **\*See page 2-22** | |  |
| **Supporting Activities** | |  |
| <<IDENTIFY HERE>> | |  |
| **Interdependencies** | |  |
| <<IDENTIFY HERE>> | |  |
| **Expected Costs** | |  |
| <<IDENTIFY HERE>> | |  |

Appendix D: Critical Systems

| **Priority** | **System Name** | **Description** | **Mission Essential Functions Supported** | **Current Location** | **Person Responsible** | **Backup (Location)** | **Testing Frequency** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| High | <<LIST CRITICAL SYSTEMS HERE>> | <<DESCRIPTION>> | <<FUNCTION>> | <<LOCATION>> | <<WHO RESPONSIBLE>> | N/A | Monthly |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Appendix E: Essential Records

| **Priority** | **Essential File, Record, or Database** | **Mission essential Functions Supported** | **Format (Hardcopy or Electronic)** | **Person Responsible** | **Pre-positioned at Alternate Facility?** | **Backup Locations or Sources?** | **Update Frequency** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| High | <<LIST ESSENTIAL RECORD HERE>> | <<DESCRIPTION>> | <<FUNCTION>> | <<LOCATION>> | <<WHO RESPONSIBLE>> | N/A | Monthly |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Appendix F: Orders of Succession and Delegations of Authority

|  |  |
| --- | --- |
| **Position** | **Line of Succession/ Delegation of Authority** |
| **Title: Agency Director** | Primary: *See Contact Appendix for Name/Contact info*  2PPndPP in Charge: Deputy Director  3PPrdPP in Charge: Operations Manager |
| **Title: Deputy Director** | Primary: *See Contact Appendix for Name/Contact info*  2PPndPP in Charge: Operations Manager  3PPrdPP in Charge: On-duty Supervisor |
| **Title: Operations Manager** | Primary: *See Contact Appendix for Name/Contact info*  2PPndPP in Charge: On-duty Supervisor |

Appendix G.1: Contact List – Agency

| **Last Name** | **First Name** | **Title** | **Office Extension or Direct #** | **Cell Number** | **Email Address** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Appendix G.2: Contact List – Member Community

| **Town / Agency** | **Last Name** | **First Name** | **Title** | **Cell Number** | **Email Address** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Appendix H: Emergency Staffing Level Response Plan

| **Level I – Normal Operations** **(0-30% FTEs are unable to work)** |
| --- |
| * <<WHAT SERVICES WILL YOU PROVIDE GIVEN STAFFING LIMITATIONS>> |
| **Level II – Limited Operations (31-50% FTEs are unable to work)** |
| * <<WHAT SERVICES WILL YOU PROVIDE GIVEN STAFFING LIMITATIONS>> |
| **Level III – Limited Operations** **(51% -70% FTEs are unable to work)** |
| * <<WHAT SERVICES WILL YOU PROVIDE GIVEN STAFFING LIMITATIONS>> |
| **Level IV – Limited Operations (71%-100%) FTEs are unable to work)** |
| * <<WHAT SERVICES WILL YOU PROVIDE GIVEN STAFFING LIMITATIONS>>   PP |

Appendix I: Business Impact Analysis Summary

Any incident that has the potential to overwhelm the typical, local response capabilities of <<INSERT AGENCY ACRONYM HERE>> is identified as a risk vulnerability. <<INSERT AGENCY ACRONYM HERE>> may need to be evacuated and relocate operations in the event of natural hazards, deliberate acts, and technological hazards.

These types of natural hazards, deliberate acts, and technological hazards, including but not limited to:

* Any type of severe weather event
* Hurricane
* Tornado
* Flooding
* Earthquake
* Public Health Emergency
* Mass Casualty Incident
* Active Assailant Incident
* Terrorist attack
* Cyber Incident
* Infrastructure Failure
* Nuclear Power Plant Incident
* Hazardous Materials Incident
* Civil Unrest
* CBRN Incident

In extreme situations, whether natural, deliberate acts, or technological hazards <<INSERT AGENCY ACRONYM HERE>> may be not being capable of maintaining a ready and operational status level.

<<INSERT AGENCY ACRONYM HERE>> may need to limit services due to employee staffing reductions during a natural hazard or deliberate act.

 The employee may not be able to get to <<INSERT AGENCY ACRONYM HERE>>, may be too ill to work, or have to self-quarantine.

**What would be the impact if the mission-essential function’s performance is disrupted?**

* 911 Emergency calls may have a delay in answer time due to call surges
* 911 Emergency calls may have a delay in answer time due to a reduction in staffing
* Radio communications may be limited or impossible due to technical issues
* Radio communications may be limited due to call surges
* Radio communications may be limited due to a reduction in staffing
* Business calls may go unanswered
* Computer-Aided Dispatch and Records Management Systems may be inaccessible.

**What is the timeframe for unacceptable loss of functions and critical assets?**

<<INSERT AGENCY ACRONYM HERE>> provides critical services to the public and public safety responders answering and processing 911 emergency calls for service, dispatching responders to emergencies, answering business line telephone calls, and providing services to member community agencies. Loss of functions and critical assets must be planned for in advance, and contingency plans must be in place in order for the minimum services disruption possible.

Risk Mitigation strategies:

<<INSERT AGENCY ACRONYM HERE>> has evacuation and relocation plans in place to respond to high-risk, low-frequency events in the event of natural hazards, deliberate acts, and technological hazards.

<<INSERT AGENCY ACRONYM HERE>> maintains a “Go Kit” in the event of the need to evacuate and relocate the operations.

<<DESCRIBE AGENCY’S POWER, UPS, PHONE, INTERNET REDUNDANCY STRATEGIES HERE>>.

Inside the communications center, there are <<XX>> answering position units (APUs). Each position is powered through one of two Uninterruptable Power Supplies (UPS). These UPSs provide backup battery power in the event of an electrical outage. Each UPS powers half of the positions. Therefore, In the event of a UPS failure, the center would only lose half of the positions.

The communications room is also powered by <<DESCRIBE HVAC REDUNDANCIES HERE>>. The center also has a robust firewall in place to prevent unauthorized intrusions into its network.

<<DESCRIBE YOUR RADIO SYSTEM AND REDUNDANT CAPABILITIES HERE>>.

In the event of an evacuation, the center would be able to utilize <<WHAT?>>.

<<DESCRIBE YOUR MUNICIPAL AND/OR CONTRACT IT SUPPORT HERE>>

<<DESCRIBE REDUNDANT CAPABILITIES FOR EACH OF YOUR MEFs HERE>>

 <<DESCRIBE ANY EMERGENCY NOTIFICATION SYSTEMS USED HERE>>.

Appendix J: Definitions

The following terms or phrases are found in this document.

***Alternate Facility***. Alternate Facilities are locations to which ERG staff can report and implement mission essential functions. Alternate Facilities must be capable of supporting operations in a threat-free environment in the event that mission essential functions and supporting staff are relocated to the site. An Alternate Facility must have sufficient space and equipment to sustain operations for a period of up to 30 days. It should also have available the telecommunication and information systems, records, and databases required to support the implementation of mission essential functions. In some cases, Alternate Facilities may not consist of physical locations but alternative work arrangements such as telework or mobile work.

***Business Impact Analysis (BIA).*** A method of identifying and evaluating the effects that various threats and hazards may have on the ability of an organization to perform its mission essential functions and the resulting impact of those effects.

***Critical Systems.*** Tasks, functions, and systems that are important to the continuation of mission essential functions. Critical systems may include but are not limited to, communications and information systems, and other specialized equipment and systems.

***Continuity Manager*.** Serves as the COOP point of contact. Responsible for coordinating the implementation of the COOP Plan; initiating appropriate notifications inside and outside the Agency/Organization during COOP Plan implementation; being the point of contact for all COOP training, testing, and exercising; assisting ERG efforts at the ERS; and initiating recovery of the Agency/Organization as part of reconstitution.

***Continuity of Operations (COOP) Plan.*** An action plan that provides for the immediate continuity of mission essential functions of an organization at an alternative facility for up to 30 days in the event an emergency prevents occupancy of its primary facility.

***Delegation of Authority.*** Delegation of authority ensures appropriate individuals are authorized to act on behalf of the organization head or other officials for specified purposes and to carry out specific duties in order to ensure an orderly transition of responsibilities. Delegations of authority will generally specify a particular function that an individual is authorized to perform and include any restrictions or limitations associated with that authority.

0T0T***Devolution.*** The transfer of statutory authority and responsibility from an organization’s primary operating staff and facilities to other staff and alternate locations to sustain essential functions when necessary.

***Emergency Relocation Group (ERG).*** Personnel0T0T identified and assigned to perform mission essential functions and deliver critical services in the event of a continuity plan activation.

***ERG Advance Team*.**  ERG personnel who immediately deploy to the Emergency Relocation Site (ERS) upon receiving a COOP warning or activation to initiate actions at the ERS in preparation for the arrival of the main body of Emergency Personnel. Advance Team plus Emergency Personnel constitute an ERG.

0T0T***Essential Records*** –Those records an organization needs to meet operational responsibilities under national security emergencies or other emergency conditions (emergency operating records) or to protect the legal and financial rights of the government and those affected by government activities (legal and financial rights records).

***Go-Kits.*** A kit prepared by and/or for an individual who expects to deploy to an alternate location during an emergency. Go-Kits should include copies of standard operating procedures, emergency plans, contact lists, and other information or guidance that is not already pre-positioned or accessible from the ERS. The ERG would take these kits to the ERS in the event of a COOP Activation.

***Hazard Identification and Risk Assessment (HIRA).*** A hazard identification and risk assessment provide a factual basis for activities proposed in the strategy portion of a hazard mitigation plan. An effective risk assessment informs proposed actions by focusing attention and resources on the greatest risks. The four basic components of a risk assessment are: 1) hazard identification, 2) profiling of hazard events, 3) inventory of assets, and 4) estimation of potential human and economic losses based on the exposure and vulnerability of people, buildings, and infrastructure.

***Mission*** 0T0T***Essential Functions (MEF).***  A subset of organizational functions that are determined to be critical activities. These functions are then used to identify supporting tasks and resources that must be included in the organization’s continuity planning process.

***Occupant Emergency Plan (OEP).*** A short-term emergency response plan which establishes procedures for evacuating buildings or sheltering-in-place in the event a situation poses a threat to the health and safety of personnel, the environment, or property. Such events include a fire, hurricane, criminal attack, or a medical emergency.

0T0T***Primary Operating Facility*** – The facility where an organization’s leadership and staff operate on a day-to-day basis.

0T0T***Reconstitution*** – The process by which surviving and/or replacement organization personnel resume normal operations.

0T0T***Recovery Time Objective.*** The targeted duration of time and a service level within which a business process must be restored after a disruption in order to avoid unacceptable consequences associated with a break in business continuity.

***Relocation Site Support Coordinator*.**  Serves as the COOP point of contact at each ERS. Responsible for the readiness and operational condition of the ERS, as appropriate, including telecommunications, infrastructure, and equipment; and support the billeting and meal needs of the ERG.

***Succession.*** A formal, sequential assumption of a position’s authorities and responsibilities by the holder of another specified position in the event of a vacancy in the office or if a position holder dies, resigns, or is otherwise unable to perform the functions and duties of that position.

***Telework.*** A work flexibility arrangement under which an employee performs the duties and responsibilities of his/her position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work.

Appendix K: Acronyms

A-Team Advance Team

AAR After Action Report

BIA Business Impact Analysis

CGC Continuity Guidance Circular

COOP Continuity of Operations

EOC Emergency Operations Center

ERG Emergency Relocation Group

ERS Emergency Relocation Site

FCD Federal Continuity Directive

GIS Geographic Information Systems

HIRA Hazard Identification and Risk Assessment

IP Implementing Procedure

IT Information Technology

MEF Mission Essential Function

MHz Megahertz

MITC Massachusetts Information Technology Center

OEP Occupant Emergency Plan

SEOC State Emergency Operations Center

SOP Standard Operating Procedure

1. Annex – Evacuation Plan

PSAP Evacuation Plan

Contents of Evacuation Plan

[PURPOSE OF PSAP EVACUATION PLAN 3-3](#_Toc85625954)

[Purpose 3-3](#_Toc85625955)

[When Activated 3-3](#_Toc85625956)

[Considerations on When to Activate the Plan 3-3](#_Toc85625957)

[Alternatives to Plan 3-4](#_Toc85625958)

[Special Considerations 3-4](#_Toc85625959)

[PSAP EVACUATION PROCEDURES 3-5](#_Toc85625960)

[Setup of Alternate/Backup PSAP Facility 3-8](#_Toc85625961)

[Appendix A. Evacuation Checklist 3-9](#_Toc85625962)

[Appendix B. Return to Normal Operations Checklist 3-10](#_Toc85625963)

[Appendix C. Go-Kits 3-11](#_Toc85625964)

[Appendix D. Recommendation for Personal Go-Kit 3-12](#_Toc85625965)

[Appendix E. Transferring Business Line Calls 3-13](#_Toc85625966)

[Appendix F. Transferring Fax Line Calls 3-14](#_Toc85625967)

[Appendix G. Toning Fire Departments from Portable Radios 3-15](#_Toc85625968)

[Appendix H. Go-Kit 3-16](#_Toc85625969)

[Setting Up IT Hardware 3-16](#_Toc85625970)

[Logging Into VPN 3-16](#_Toc85625971)

[Wireless Router Settings 3-16](#_Toc85625972)

[Appendix I. Important Numbers, Password, and other Information 3-17](#_Toc85625973)

[Appendix J. Setting up Radio Console at Alt. Location 3-18](#_Toc85625974)

[Appendix K. Evacuation Routes / Rally Point Locations 3-19](#_Toc85625975)

[Appendix L. Go-Kits Monthly Checklist 3-20](#_Toc85625976)

PURPOSE OF PSAP EVACUATION PLAN

Purpose

1. Designed to assist supervisory and administrative staff with the appropriate steps to be utilized in the event of a PSAP evacuation.
2. Provide guidance that aligns with the center’s Emergency Operation Plan, and its associated annexes including the continuity of operations plan (COOP).

When Activated

1. When ordered to evacuate by a public safety Incident Commander (Police/Fire/EMS) or <<INSERT AGENCY ACRONYM HERE>> Administrator/Supervisor;
2. Unable to staff the facility for any reason;
3. Visible smoke or visible flames in the building;
4. Chemical spill and/or release of hazardous materials in/on/near building causing need to evacuate;
5. Potential hazardous situation causing employees to become sick;
6. An explosion in the building causing a need to evacuate;
7. No electricity and generator will not start; or
8. Bomb or suspicious device located in/near the Building

Considerations on When to Activate the Plan

1. **Event With Warning**
   1. Is the threat aimed at the facility or surrounding area?
   2. Is the threat aimed at organization personnel?
   3. Are employees unsafe remaining in the facility and/or area?
   4. Who should be notified of the threat?
   5. Is it safe for employees to return to work the next day?
2. **Event Without Warning**
   1. Is the facility affected?
   2. Are personnel affected?
   3. Have personnel safely evacuated, or are they sheltering-in-place?
   4. What are the instructions from first responders?
   5. How soon must the organization be operational?

### Plan When PSAP Affected by partial/full loss of on-duty Personnel

1. 911 and Radio functions to be assumed by Alternative PSAP until <<INSERT AGENCY ACRONYM HERE>> off-duty staff arrives at Alternate or Backup PSAP and is able to resume operations

Alternatives to Plan

The Plan will be adapted as conditions necessitate. For example:

1. Very Short-term evacuation (e.g., less than 1 hour)
   1. May be able to operate outside or nearby until the facility is checked and declared safe for re-entry.
   2. May only need to send one (1) telecommunicator to the Alternate PSAP location

### Available Resources

1. Alternative PSAP
   1. <<WHO/WHERE? >>.
2. Backup PSAP
   1. <<WHO/WHERE? >>.
3. <<OTHER RESOURCES >>.

Special Considerations

Operating the PSAP with diminished capacity (e.g., don’t evacuate but deal with no radio consoles, or no 911 phones but all other phones, etc.).

PSAP EVACUATION PROCEDURES

1. **Initial Evacuation Steps**
   1. PSAP Supervisor assesses threat, makes the decision to evacuate with approval of <<INSERT AGENCY ACRONYM HERE>> Director (if time permits), and decides on the Rally point (e.g., the Essex Sports Center) **[See page 3-19 for more information]**
   2. Supervisor announces evacuation order and Rally Point to all personnel in the building
   3. Perform key tasks by position if time permits
      1. these tasks are performed with the most important being listed at the top
      2. **SEE page 3-9**
      3. **Evacuation** Checklist
   4. Terminate all in-progress 911 calls rapidly (transfer any to Alternate PSAP that need continued attention). Do not answer ringing phones.
   5. SAFETY FIRST, GET OUT, AND MAKE NOTIFICATIONS LATER!!!
2. **Post-Evacuation / Rally Point**
   1. Count all staff and assure that each member is safe and accounted for
3. **On-Duty Supervisor Responsibilities**
   1. Go over the list of tasks on **page 3-9**
   2. Evacuation Checklist and perform any that did not get performed while at Rally Point (using cell phones and portable radios)
   3. Split personnel into two groups:
      1. Telecommunicators to Alternate PSAP
   4. Arrange vehicles for the transport of <<INSERT AGENCY ACRONYM HERE>> staff to Alternate and/or Backup PSAP.
      1. Possible transportation considerations may include:
         1. Personal Owned Vehicle (POV); or
         2. <<OTHER OPTIONS>>
   5. Notify all employees of evacuation (Use Emergency Notification System to send alert – **See page 3-17 for Important Numbers**)
      1. 1 Member of Administration – Report to Alternate PSAP
      2. Reschedule next shift to report to the appropriate alternate or backup PSAP
   6. Supervisor notifies NG911 Provider to advise of Primary PSAP evacuation and to route calls to designated Alternate PSAP.
   7. Building Security
      1. Upon evacuating the building, if it is safe to do so, ensure that the building is secured behind you.
4. **On-Duty Telecommunicator Responsibilities**
   1. Telecommunicator makes Notification to member police and fire departments on ALL police/fire channels of transitional PSAP operation while the staff is in transit to the alternate/backup PSAP location.
      1. Advise police/fire units: “**[ALTERNATE PSAP PERSONNEL] ARE HANDLING REGIONAL’S 911 CALLS AND WILL NOTIFY PSAP PERSONNEL ON <<IDENTIFY CHANNEL HERE>> OF ANY CALLS FOR SERVICE; CALLS TO ALL BUSINESS LINES WILL RECEIVE NO ANSWER UNTIL RE-ROUTED BY <<INSERT AGENCY ACRONYM HERE>> STAFF WHEN ABLE TO DO SO. MORE INFORMATION TO FOLLOW AFTER WE RELOCATE DISPATCHERS TO OUR ALTERNATE SITE. ALL DEPARTMENTS PLEASE LIMIT RADIO TRANSMISSIONS TO EMERGENCY TRAFFIC ONLY (REPEAT 2x).**”
      2. Conduct Rollcall with each member police and fire department to confirm receipt of the message (if time allows).
   2. Telecommunicator makes notification on **<<IDENTIFY CHANNEL HERE>>** to notify surrounding cities and towns of the evacuation.
      1. Advise: “**<<INSERT AGENCY NAME HERE>> TO SURROUNDING CITIES AND TOWNS, SPECIAL ATTENTION <<IF APPLICABLE>>, BE ADVISED THE <<INSERT AGENCY ACRONYM HERE>> CENTER HAS EVACUATED FROM OUR FACILITY. 911 CALLS WILL BE ROUTED TO OUR ALTERNATES: <<IDENTIFY ALTERNATE HERE>>. CALLS TO ALL BUSINESS LINES WILL RECEIVE NO ANSWER UNTIL RE-ROUTED BY <<INSERT AGENCY ACRONYM HERE>> STAFF WHEN ABLE TO DO SO. MORE INFORMATION TO FOLLOW AFTER WE RELOCATE DISPATCHERS TO OUR ALTERNATE SITE. (REPEAT 2x)**”

Setup of Alternate/Backup PSAP Facility

### Alternate PSAP

<<DESCRIBE ALTERNATE PSAP HERE>>

**Setup Plan**

1. <<IDENTIFY EACH MEF SYSTEM AND THE PROCESS OF LOGGING INTO THEM HERE>>
2. **Miscellaneous**
   1. Obtain paper, pencils, pens, etc., from the Go-Kit and place with the above positions
   2. Develop a plan for police and fire unit status boards, if needed (whiteboards). May need to improvise.

1. Evacuation Checklist

### On-Duty Telecommunicator Duties:

Make Radio Announcement and send MDT message to Member Communities

Advise <<IF APPLICABLE>> of Need to monitor fire alarms

Priority Radio message to <<YOUR ALTERNATE PSAP>> via <<RADIO CHANNEL>>

### On-Duty Supervisor Duties:

Grab Go-Kits, all portable radios, & PSAP Supervisor’s cell phone

Take a screenshot of all active/pending police and fire calls

Ask all staff to bring any personal cell phones

Grab PSAP roster for the current shift

Ensure all personnel have exited the building safely

Review Telecommunicator’s Checklist

Notify 911 provider to move 911 Calls to Alternate

Off Duty Staff notified (Emergency Notification System)

CJIS / OpenFox Application Terminal (Route to Alternate location)

Relocate unassigned personnel

Notify contract ambulance services

### <<INSERT AGENCY ACRONYM HERE>> Administration Duties

Notify all advisory board members

Review Supervisor’s Checklist

Coordinate/Assign Administrative/IT Staff

PIO Message

Remote sites notified/staffed/operations

Radios tested

Law Enforcement terminal forwarded

Staff Accounted for and assigned

Consider notifying Local Emergency Management, if needed

Consider using ARES/RACES, if needed

### IT Personnel Duties

Technical Staff Responding

IP Connectivity

Radios Operational

Phones Operational

1. Return to Normal Operations Checklist

### On-Duty Supervisor/Telecommunicator Duties

Assign staff to return to Communications Center

Notify 911 provider to move 911 Calls back to <<INSERT AGENCY ACRONYM HERE>>

Notify Departments via Radio and MDT message of resuming normal operations

Notify surrounding towns of return to normal operations

Notify CJIS to return CJIS / OpenFox messages to <<INSERT AGENCY ACRONYM HERE>>

IP Connectivity

Account for personnel

Relocate unassigned personnel

### <<INSERT AGENCY ACRONYM HERE>> Administration Duties

Ensure the safety of Communications Center personnel

Technical Manager ensures system operational

Verify On-Duty Supervisor/Telecommunicator Duties are completed

Communications Center notified/staffed/operational

PIO Message

Radios tested

Verify Law Enforcement terminal returned to <<INSERT AGENCY ACRONYM HERE>>

Staff Accounted for and assigned or released

Notify all advisory board members

Notify Local Emergency Management?

Notify ARES/RACES?

After-action report completed

### IT Personnel Duties

All systems operational

Notify Director that Communications Center Operational

Release technicians

1. Go-Kits

**Contents**

* Pelican
* Emergency Operations Plan (EOP)
* Copies of Essential Records (**See page 2-26 for a list of contents**)
* Portable Radios
  + VHF Radio
  + UHF Radio
  + Radio Charger
  + Extra Battery, if possible
* Laptop Computers (Qty. 2)
* EMD Cards: 1 set
* MDC Identifier List
* Supervisor’s Cell Phone
* Flashlight
* Business and personal contact numbers
  + Emergency phone numbers and addresses (relatives, medical doctor, pharmacist)
* Chargers/extra batteries for phones, GPS, and laptop
* Bottled water and non-perishable food (i.e., granola, dried fruit, etc.)
* First Aid Supply Kit
* optional:
  + Personal Cell Phones: as many as possible

1. Recommendation for Personal Go-Kit

* Identification and charge cards
  + <<INSERT AGENCY ACRONYM HERE>> Identification
  + Driver’s license
  + Health insurance card
  + Personal charge card
  + Cash
* Communication equipment
  + Cell phone & Charger
* Change of clothes
* Flashlight
* Personal contact numbers
  + Emergency phone numbers and addresses (relatives, medical doctor, pharmacist)
* Toiletries
* Chargers/extra batteries for phone or laptop
* Bottled water and non-perishable food (i.e., granola, dried fruit, etc.)
* Medical needs
  + Insurance information
  + List of allergies/blood type
  + Hearing aids and extra batteries
  + Glasses and contact lenses
  + Extra pair of eyeglasses/contact lenses
  + Prescription drugs (30-day supply)
  + Over-the-counter medications, dietary
* supplements
* [Insert additional recommended items]

1. Transferring Business Line Calls
2. <<DESCRIBE IN-DEPTH ON HOW TO TRANSFER YOUR BUSINESS LINES CALLS STEP-BY-STEP HERE>>
3. <<DESCRIBE IN-DEPTH ON HOW TO RETURN YOUR BUSINESS LINES CALLS STEP-BY-STEP TO NORMAL OPERATIONS HERE>>
4. Transferring Fax Line Calls
5. <<DESCRIBE IN-DEPTH ON HOW TO TRANSFER YOUR FAX LINES STEP-BY-STEP HERE>>
6. <<DESCRIBE IN-DEPTH ON HOW TO RETURN YOUR FAX LINES STEP-BY-STEP TO NORMAL OPERATIONS HERE>>
7. Toning Fire Departments from Portable Radios

<<DESCRIBE HOW YOU WOULD ACTIVATE FIRE DEPARTMENTS FROM MOBILE AND/OR PORTABLE RADIOS. INCLUDE PICTURES AND STEP-BY-STEP GUIDE HERE>>

1. Go-Kit

Setting Up IT Hardware

1. <<DESCRIBE IN-DEPTH ON HOW TO SET UP GO-KIT TECHNOLOGY EQUIPMENT LIKE ROUTERS, COMPUTERS, CRADLEPOINTS, ETC., INCLUDING PICTURES HERE>>

Logging Into VPN

1. <<DESCRIBE IN-DEPTH ON HOW TO ACCESS YOUR LOCAL NETWORK REMOTELY, INCLUDING STEP-BY-STEP PICTURES/PASSWORDS HERE>>

Wireless Router Settings

<<LIST EACH WIRELESS ACCESS DEVICE HERE INCLUDING ALL REQUIRED CREDENTIALS, IP ADDRESS, SUBNET, DESCRIBE IN-DEPTH ON HOW TO ACCESS YOUR LOCAL NETWORK REMOTELY, INCLUDING STEP-BY-STEP PICTURES/PASSWORDS HERE>>

* Admin Website:
* Admin Username:
* Admin Password:
* WiFi Network SSID:
* WiFi Password:
* IP Range:
* External IP Address:

1. Important Numbers, Password, and other Information
2. **Important Numbers**
   1. <<LIST HERE >>
3. **Important Password**
   1. <<LIST HERE >>
4. **Conference Calls**
   1. Host Instructions
      1. <<LIST HERE >>
   2. **Participant Instructions**
      1. <<LIST HERE >>
5. **Swiftreach – Emergency Notification System**
   1. <<LIST EACH WIRELESS ACCESS DEVICE HERE INCLUDING ALL REQUIRED CREDENTIALS, IP ADDRESS, SUBNET, DESCRIBE IN-DEPTH ON HOW TO ACCESS YOUR LOCAL NETWORK REMOTELY, INCLUDING STEP-BY-STEP PICTURES/PASSWORDS HERE>>

1. Setting up Radio Console at Alt. Location

<<DESCRIBE HOW TO ACCESS YOUR RADIO SYSTEM FROM ALTERNATE PSAP, INCLUDING STEP-BY-STEP PICTURES/PASSWORDS HERE>>

1. Evacuation Routes / Rally Point Locations

<<INSERT A MAP HERE TO SHOW YOUR SITE WITH EVACUATION ROUTE AND RALLY POINT(S) >>

1. Go-Kits Monthly Checklist

**All items identified on page 3-11 shall be checked monthly to ensure that batteries are charged, electronics are functioning properly, the software is up-to-date, non-electronic items are functioning properly, and necessary inventory is maintained.**

| **Date Checked (MM/DD/YYYY)** | **Name of Person Checking** | **Initials** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. Annex – Site Map

The following sections contain an aerial map and building schematics of the <<INSERT AGENCY ACRONYM HERE>> Facility.

<<INSERT SITE MAP HERE >>

<<INSERT BUILDING SCHEMATICS HERE >>

**Room Identification Index**

| **Room Number** | **Description** | **Room Number** | **Description** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Annex – Critical Infrastructure Shutoff Locations

The following section contains a map depicting the locations of Critical Infrastructure, and a step-by-step process to shut off the building utilities at the <<INSERT AGENCY ACRONYM HERE>> Facility.

**Critical Infrastructure Locations**

<<INSERT A MAP HERE SHOWING CRITICAL INFRASTRUCTURE LOCATIONS>>

**Power**

Shutting down power:

<<DESCRIBE HOW TO SHUT DOWN BUILDING POWER WITH PICTURES >>

Restoring power:

<<DESCRIBE HOW TO RESTORE BUILDING POWER WITH PICTURES >>

**Water**

Shutting off water:

1. <<DESCRIBE HOW TO SHUT DOWN WATER WITH PICTURES >>

**Gas**

Shutting gas off:

<<DESCRIBE HOW TO SHUT DOWN GAS WITH PICTURES>>

Figure 6: Gas Shutoff Valve

1. Annex – Radio Communications (ICS-217, QC-II, and DTMF Tones)

The following section contains a listing of all <<INSERT AGENCY ACRONYM HERE>> Member Agencies’ Frequencies, and any associated Quick Call – II (QC-II) or DTMF Tones.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **COMMUNICATIONS RESOURCE AVAILABILITY WORKSHEET** | | | | | | **Frequency Band** | | **Description** | |
|  | | | | |  | | | | |
|  | **Channel Configuration** | **Channel Name/Trunked Radio System Talkgroup** | **Eligible Users** | **RX Freq N or W** | **RX Tone/NAC** | **TX Freq N or W** | **Tx Tone/NAC** | **Mode A, D or M** | **Remarks** |
| **1** |  |  |  |  |  |  |  |  |  |
| **2** |  |  |  |  |  |  |  |  |  |
| **3** |  |  |  |  |  |  |  |  |  |
| **4** |  |  |  |  |  |  |  |  |  |
| **5** |  |  |  |  |  |  |  |  |  |
| **6** |  |  |  |  |  |  |  |  |  |
| **7** |  |  |  |  |  |  |  |  |  |
| **8** |  |  |  |  |  |  |  |  |  |
| **9** |  |  |  |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |  |  |  |
| **11** |  |  |  |  |  |  |  |  |  |
| **12** |  |  |  |  |  |  |  |  |  |
| **13** |  |  |  |  |  |  |  |  |  |
| **14** |  |  |  |  |  |  |  |  |  |
| **15** |  |  |  |  |  |  |  |  |  |
| **16** |  |  |  |  |  |  |  |  |  |
| **17** |  |  |  |  |  |  |  |  |  |
| **18** |  |  |  |  |  |  |  |  |  |
| **19** |  |  |  |  |  |  |  |  |  |
| **20** |  |  |  |  |  |  |  |  |  |

**The convention calls for frequency lists to show four digits after the decimal place, followed by either an “N” or a “W”, depending on whether the frequency is narrow or wide band. Mode refers to either “A” or “D” indicating analog or digital (e.g., Project 25) or “M” indicating mixed mode. All channels are shown as if programmed in a control station, mobile or portable radio. Repeater and base stations must be programmed with the Rx and Tx reversed.**

**Quick Call – II Tones**

| **Quick Call – II Tones** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Town** | **Tone Name** | **Tone A** | **Tone B** | **Motorola Code** | **Notes** |
|  |  |  | | |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  | | |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |

**DTMF Tones**

| **DTMF Tones** | | | | |
| --- | --- | --- | --- | --- |
| **Town** | **Department** | **Function** | **Tone** | **Notes** |
|  |  |  |  |  |
|  |  |  |
|  |  |  |  |
|  |  |  |

1. Annex – Emergency Onboarding of PSAP into <<INSERT AGENCY ACRONYM HERE>>

In the event that another PSAP needs to be onboarded into <<INSERT AGENCY ACRONYM HERE>> due to an emergency, like a pandemic flu, the following checklist should be used.

* 911 System
* Telephone (Non-Emergency) System
* Computer-Aided Dispatch (CAD)
  + Items Needed
  + The community’s IT Contact name, number, and email.
  + Limitations
  + If time allows
    - List of utility company’s & their contact numbers
    - List of DPW & ACO Contacts
    - List of inspector numbers
    - List of fire hydrants?
    - List of Fire line boxes, if used and available
    - List of specialty facilities (healthcare, hazardous, etc.)
    - List of intersections?
* Radio System
  + Can they use one of our member department frequencies?
    - If yes
      * Assign to that frequency
    - If no
      * Consider using …

1. Annex – Document Templates

The following sections contain a listing of available document templates.

**Document Templates**

<<DESCRIBE AVAILABLE TEMPLATES AND WHERE THEY RESIDE HERE>>

1. Hazard- and Threat-Specific Annexes

The following sections contain Hazard- and Threat-Specific Annexes.

**Hazard- and Threat-Specific Annexes**

These annexes do not repeat content but rather build on the information within the basic plan.

1. Annex – Threat/Actual Violence at or Near Workplace Plan

The following section contains the <<INSERT AGENCY ACRONYM HERE>> Threat/Actual Violence at or Near Workplace Plan.

**Threat/Actual Violence at or Near Workplace Plan**

A threat or act of violence at or near <<INSERT AGENCY ACRONYM HERE>> may be received through numerous means. For the purposes of this plan, the term “near” shall mean <<DESCRIBE>>. Specifically included are <<IDENTIFY NEIGHBORING BUILDINGS/BUSINESSES THAT MAY BE INCLUDED HERE>>.

When performing a risk assessment, <<INSERT AGENCY ACRONYM HERE>> should consider the following:

* How did the business become aware of the threat?
  + 911 call to PSAP
  + Non-Emergency call to PSAP
  + Telephone call to Business
  + Called into the business directly
  + Texted to employee at the business
  + Email message
  + Threat written/posted at or in the business

In the event of a threat or actual violence incident at or near the <<INSERT AGENCY ACRONYM HERE>> facility, the following plan should be utilized.

**On-Duty Supervisor Responsibilities**

1. <<DESCRIBE RESPONSIBILITIES>>.

**<<INSERT AGENCY ACRONYM HERE>> Administrative Personnel**

1. <<DESCRIBE RESPONSIBILITIES>>.

**On Duty <<INSERT AGENCY ACRONYM HERE>> Telecommunicator Staff**

1. <<DESCRIBE RESPONSIBILITIES>>.
2. Annex – Cybersecurity Incident Handling Plan

Cybersecurity Incident Handling Plan

Contents of Cybersecurity Incident Handling Plan

[INTRODUCTION C-4](#_Toc85625977)

[Purpose and Scope C-4](#_Toc85625978)

[Concept of Operations C-4](#_Toc85625979)

[Overview C-4](#_Toc85625980)

[Events and Incidents C-4](#_Toc85625981)

[Need for Incident Response C-5](#_Toc85625982)

[Handling an Incident C-5](#_Toc85625983)

[Preparation C-6](#_Toc85625984)

[Preparing to Handle Incidents C-6](#_Toc85625985)

[Preventing Incidents C-7](#_Toc85625986)

[Detection and Analysis C-9](#_Toc85625987)

[Attack Vectors C-9](#_Toc85625988)

[Signs of an Incident C-10](#_Toc85625989)

[Sources of Precursors and Indicators C-11](#_Toc85625990)

[Incident Analysis C-12](#_Toc85625991)

[Incident Documentation C-15](#_Toc85625992)

[Incident Prioritization C-15](#_Toc85625993)

[Incident Notification C-18](#_Toc85625994)

[Containment, Eradication, and Recovery C-19](#_Toc85625995)

[Choosing a Containment Strategy C-19](#_Toc85625996)

[Evidence Gathering and Handling C-20](#_Toc85625997)

[Identifying the Attacking Hosts C-20](#_Toc85625998)

[Eradication and Recovery C-21](#_Toc85625999)

[Post-Incident Activity C-22](#_Toc85626000)

[After-Action Review C-22](#_Toc85626001)

[Using Collected Incident Data C-23](#_Toc85626002)

[Evidence Retention C-25](#_Toc85626003)

[Coordination and Information Sharing C-25](#_Toc85626004)

[Coordination C-26](#_Toc85626005)

[Sharing Agreements and Reporting Requirements C-26](#_Toc85626006)

[Information Sharing Techniques C-27](#_Toc85626007)

[Incident Response Partners (Vendors, State, Federal) C-27](#_Toc85626008)

[Vendors C-27](#_Toc85626009)

[State C-27](#_Toc85626010)

[Federal C-27](#_Toc85626011)

[Plan Maintenance & Testing C-28](#_Toc85626012)

[Plan Maintenance C-28](#_Toc85626013)

[Testing C-28](#_Toc85626014)

[Cyber Incident Response Plan C-29](#_Toc85626015)

[Overview C-29](#_Toc85626016)

[Questions to Consider C-29](#_Toc85626017)

[Active Incident Considerations C-30](#_Toc85626018)

[Appendix A. Reporting Incidents C-32](#_Toc85626019)

[Appendix B. Roles of State/Federal Cybersecurity Centers C-35](#_Toc85626020)

[Appendix C. Core Capabilities and Critical Tasks C-37](#_Toc85626021)

[Appendix D. Additional Resources C-41](#_Toc85626022)

[Appendix E. Acronyms C-43](#_Toc85626023)

[Appendix F. Incident Handling Checklist C-45](#_Toc85626024)

INTRODUCTION

Purpose and Scope

This document seeks to mitigate risks from computer security incidents by providing practical guidelines on responding to incidents effectively and efficiently. It includes guidelines on establishing an effective incident response program. The primary focus of this document is detecting, analyzing, prioritizing, and handling incidents.

Cyber incident response is an important component of information and communications technology (ICT) and operational technology programs and systems. Performing incident response effectively is a complex undertaking and requires substantial planning and resources.

This document is the strategic framework for operational coordination among <<INSERT AGENCY ACRONYM HERE>>, the private sector, and our partners (<<INSERT AGENCY ACRONYM HERE>> IT Team). It sets forth a Cyber Security Incident Handling Plan that creates the strategic framework for how <<INSERT AGENCY ACRONYM HERE>> plans, prepares and responds to cyber incidents. It establishes an architecture for coordinating the broader community response during a significant cyber incident in conjunction with federal, state, and/or local laws or agency policy. This IRP is also designed to integrate and interface with industry standards and best practices for cybersecurity risk management, as developed by the National Institute of Standards and Technology’s (NIST) Framework for Improving Critical Infrastructure Cybersecurity. The Incident Response Plan (IRP) is detailed on **page C-29**.

Concept of Operations

Overview

This document serves as <<INSERT AGENCY ACRONYM HERE>>’s Cyber Security Incident Handling Plan. It addresses several major decisions and actions. One of the first considerations is to identify the term “incident” so that the scope of the term is clear. This includes what services, or actions, the <<INSERT AGENCY ACRONYM HERE>> IT Team should provide.

Events and Incidents

A **cyber-security event** is any observable occurrence on a computer system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.

***Adverse cyber-security events*** are events with negative consequences, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. This guide addresses only adverse events that are computer security-related, not those caused by natural disasters, power failures, etc.

A ***cyber-security incident*** is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents are:

* An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
* Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
* An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
* A user provides or exposes sensitive information to others through peer-to-peer file-sharing services.

Need for Incident Response

Attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when security breaches occur. <<INSERT AGENCY ACRONYM HERE>> shall have an incident response capability that supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken.

Incident response helps personnel to minimize loss or theft of information and disruption of services caused by incidents. It also provides the ability to use information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data. An incident response capability also helps when dealing with legal issues that may arise during incidents.

Handling an Incident

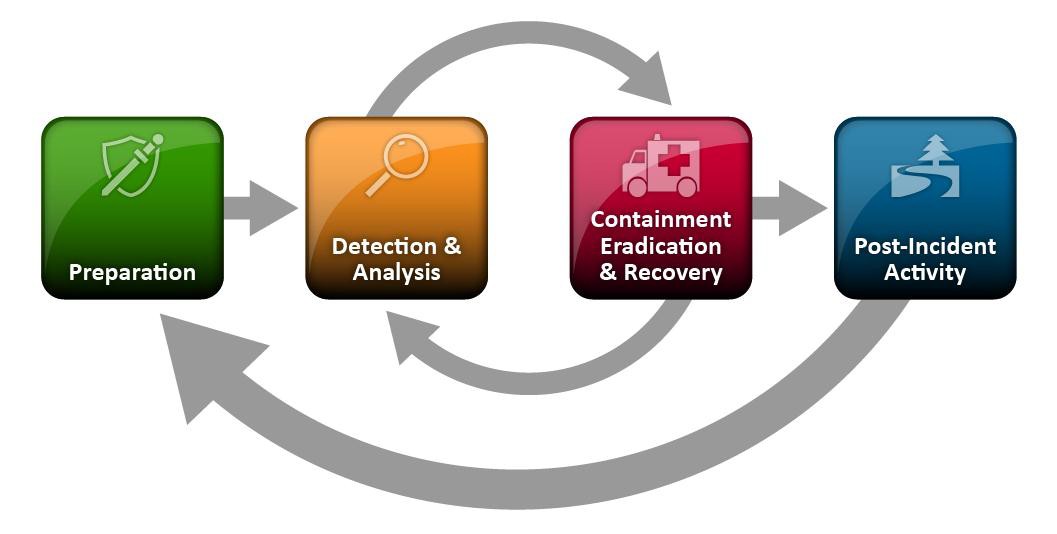
The incident response process has several phases.

1. The initial step involves establishing and training an <<INSERT AGENCY ACRONYM HERE>> IT Team (<<INSERT AGENCY ACRONYM HERE>> IT Team) and acquiring the necessary tools and resources.
2. During preparation, the organization also attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. Residual risk will inevitably persist after controls are implemented.
3. Detection of security breaches is necessary to alert the organization whenever incidents occur.
4. In keeping with the severity of the incident, the organization can mitigate the impact of the incident by containing it and ultimately recovering from it. During this phase, the activity often cycles back to detection and analysis—for example, to see if additional hosts are infected by malware while eradicating a malware incident.
5. After the incident is adequately handled, the organization should issue a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents.

The above describes the major phases of the incident response process—preparation, detection and analysis, containment, eradication and recovery, and post-incident activity—in detail. Figure 3‑1 illustrates the incident response life cycle.

***One of the challenges with handling an incident is detecting a breach. The average time to identify a data breach is six (6) months.***

Figure Error! No text of specified style in document.‑1 Incident Response Life Cycle



Preparation

Incident response methodologies typically emphasize preparation—not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. This section provides the basic direction <<INSERT AGENCY ACRONYM HERE>> shall follow when preparing to handle incidents and on preventing incidents.

To better prepare for a cyber-attack, <<INSERT AGENCY ACRONYM HERE>> has developed a multi-pronged approach:

1. Review and update policies that deter an incident from happening within its operating systems;
2. Review and update policies that deter an incident from happening within its network;
3. Launching discovery tools to detect if a breach is happening; and
4. Deploying a Rapid Response Framework to manage an incident when one occurs.

Preparing to Handle Incidents

The lists below provide tools and resources that may be of value during an incident. These lists are intended to be a starting point and may vary depending on the type of incident. For example, smartphones are one way to have resilient emergency communication and coordination mechanisms.

Incident Analysis Resources:

* Port lists, including commonly used ports and Trojan horse ports
* Documentation for OSs, applications, protocols, and intrusion detection, and antivirus products
* Network diagrams and lists of critical assets, such as database servers
* Current baselines of the expected network, system, and application activity
* Cryptographic hashes of critical files[[1]](#footnote-2) to speed incident analysis, verification, and eradication

Incident Mitigation Software:

* Access to images of clean OS’s and application installations for restoration and recovery purposes
* Snapshots of Server OS’s

<<INSERT AGENCY ACRONYM HERE>> has developed a jump kit that should be used in the event of an incident. The jump kit is contained within and a part of the agency’s Go-Kit. It includes specific computer software that can be used during incident response to detect, identify, or mitigate an incident. It includes materials that may be needed during an investigation and is ready to go at all times. The Go-Kit contains many of the items listed in the bulleted lists above.

The Go-Kit should include at least two computing devices (e.g., laptops). One should be used to perform packet sniffing, malware analysis, and all other actions that risk contaminating the computer that performs them. This laptop should be scrubbed, and all software reinstalled before it is used for another incident. The other laptop would allow for writing reports, reading emails, and performing other duties unrelated to the hands-on incident analysis.

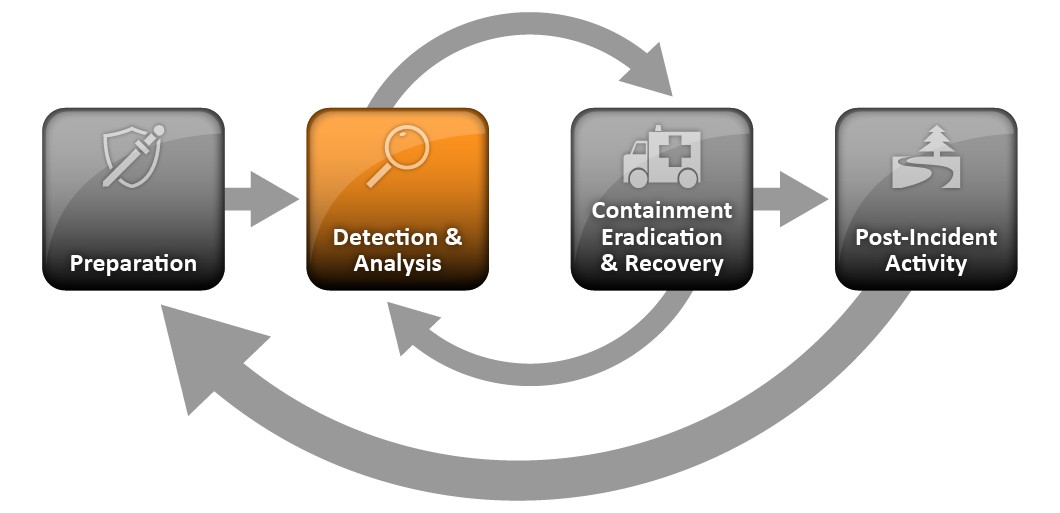
Preventing Incidents

Keeping the number of incidents to a minimum is very important to protect <<INSERT AGENCY ACRONYM HERE>> processes. If security controls are insufficient, higher volumes of incidents may occur, overwhelming the <<INSERT AGENCY ACRONYM HERE>> IT Team. This can lead to slow and incomplete responses, which translate to a more substantial negative impact (e.g., more extensive damage, longer periods of service, and data unavailability).

To prevent attacks, <<INSERT AGENCY ACRONYM HERE>> has taken the following steps to secure its network, systems, and applications:

* **Risk Assessments**. Periodic risk assessments of systems and applications are conducted to determine what risks are posed by combinations of threats and vulnerabilities.[[2]](#footnote-3) This includes understanding the applicable threats, including organization-specific threats. Each risk should be prioritized, and the risks can be mitigated, transferred, or accepted until a reasonable overall level of risk is reached. Another benefit of conducting risk assessments regularly is that critical resources are identified, allowing staff to emphasize monitoring and response activities for those resources.[[3]](#footnote-4)
* **Host Security**. All hosts have been hardened appropriately using standard configurations. In addition to keeping each host properly patched, hosts have been configured to follow the principle of least privilege—granting users only the privileges necessary for performing their authorized tasks. Hosts have auditing enabled and log significant security-related events. The security of hosts and their configurations should be continuously monitored.[[4]](#footnote-5) <<INSERT AGENCY ACRONYM HERE>> also uses the Security Content Automation Protocol (SCAP)[[5]](#footnote-6) expressed operating system and application configuration checklists to assist in securing hosts consistently and effectively.[[6]](#footnote-7)
  + Host-based firewall
  + Security Content Automation Protocol
* **Network Security**. The network perimeter has been configured to deny all activity that is not expressly permitted.
  + <<DESCRIBE STEPS YOUR AGENCY IS TAKING TO PROTECT ITS NETWORK HERE>>.
* **Malware Prevention**. Software to detect and stop malware should be deployed throughout the organization. Malware protection should be deployed at the host level (e.g., server and workstation operating systems), the application server level (e.g., email server, web proxies), and the application client level (e.g., email clients, instant messaging clients).[[7]](#footnote-8)
  + Malware Protection – <<DESCRIBE YOUR MITIGATION STRATEGIES HERE>>.
* **User Awareness and Training**. Users should be made aware of policies and procedures regarding the appropriate use of networks, systems, and applications. Applicable lessons learned from previous incidents should also be shared with users so they can see how their actions could affect the organization. Improving user awareness regarding incidents should reduce the frequency of incidents. <<INSERT AGENCY ACRONYM HERE>> IT should be trained so that they can maintain their networks, systems, and applications in accordance with the organization’s security standards.
  + <<DESCRIBE YOUR MITIGATION STRATEGIES HERE>>.
  + Exercises involving simulated incidents should be practiced for preparing <<INSERT AGENCY ACRONYM HERE>> for incident handling; see NIST SP 800-84 for more information on exercises[[8]](#footnote-9).

Detection and Analysis



Incident Detection and Analysis

Attack Vectors

Incidents can occur in countless ways. It is not feasible to develop step-by-step instructions for handling every incident. <<INSERT AGENCY ACRONYM HERE>> should plan and prepare to handle any incident, with special attention on incidents that use common attack vectors.

The attack vectors listed below are not intended to provide a definitive classification for incidents; instead, they contain conventional methods of attack, which can be used as a basis for defining more specific handling procedures. <<INSERT AGENCY ACRONYM HERE>> shall understand that different types of incidents merit different response strategies.

* **External/Removable Media**: An attack executed from removable media or a peripheral device—for example, malicious code spreading onto a system from an infected USB flash drive.
* **Attrition**: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a DDoS intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, CAPTCHAS, or digital signatures).
* **Web**: An attack executed from a website or web-based application—for example, a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware.
* **Email**: An attack executed via an email message or attachment—for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message.
* **Impersonation**: An attack involving the replacement of something benign with something malicious— for example, spoofing, a man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
* **Improper Usage**: Any incident resulting from a violation of an organization’s acceptable usage policies by an authorized user, excluding the above categories; for example, a user installs file-sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
* **Loss or Theft of Equipment**: The loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token.
* **Other**: An attack that does not fit into any of the different categories.

Signs of an Incident

The most challenging part of the incident response process is accurately detecting and assessing possible incidents—determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem. What makes this so challenging is a combination of these three factors:

1. Incidents may be detected through many different means, with varying levels of detail and fidelity. Automated detection capabilities include network-based and host-based IDPSs, antivirus software, and log analyzers. Incidents may also be detected through manual means, such as problems reported by users. Some incidents have overt signs that can be easily detected, whereas others are almost impossible to detect.
2. The volume of potential signs of incidents is typically high. For example, it is not uncommon for an organization to receive thousands or even millions of intrusion detection sensor alerts per day. (See **page C-12** for information on analyzing such alerts.)
3. In-depth, specialized technical knowledge and extensive experience are necessary for the proper and efficient analysis of incident-related data.

Signs of an incident fall into one of two categories: precursors and indicators. A ***precursor*** is a sign that an incident may occur in the future. An ***indicator*** is a sign that an incident may have happened or may be occurring now.

Most attacks do not have any identifiable or detectable precursors from the target’s perspective. If precursors are detected, the <<INSERT AGENCY ACRONYM HERE>> IT Team may have an opportunity to prevent the incident by altering its security posture to save a target from attack. At a minimum, the <<INSERT AGENCY ACRONYM HERE>> IT Team could monitor activity involving the target more closely. Examples of precursors are:

* Web server log entries that show the usage of a vulnerability scanner
* An announcement of a new exploit that targets a vulnerability of the organization’s mail server
* A threat from a group stating that the group will attack the organization.

While precursors are relatively rare, indicators are all too common. Too many types of indicators exist to list, but some examples are listed below:

* A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server.
* Antivirus software alerts when it detects that a host is infected with malware.
* A system administrator sees a filename with unusual characters.
* A host records an auditing configuration change in its log.
* An application logs multiple failed login attempts from an unfamiliar remote system.
* An email administrator sees a large number of bounced emails with suspicious content.
* A network administrator notices an unusual deviation from typical network traffic flows.

Sources of Precursors and Indicators

Precursors and indicators are identified using many different sources, with the most common being computer security software alerts, logs, publicly available information, and people.

The table below lists common sources of precursors and indicators for each category.

Common Sources of Precursors and Indicators

| **Source** | **Description** |
| --- | --- |
| **Alerts** | |
| **IDPSs** | IDPS products identify suspicious events and record pertinent data regarding them, including the date and time the attack was detected, the type of attack, the source and destination IP addresses, and the username (if applicable and known). Most IDPS products use attack signatures to identify malicious activity; the signatures must be kept up to date so that the newest attacks can be detected. IDPS software often produces *false positives*—alerts that indicate malicious activity is occurring, when, in fact, there has been none. Analysts should  manually validate IDPS alerts either by carefully reviewing the recorded supporting data or by getting related data from other sources.[[9]](#footnote-10) |
| **SIEMs** | Security Information and Event Management (SIEM) products are similar to IDPS products, but they generate alerts based on the analysis of log data (see below). |
| **Antivirus and antispam software** | Antivirus software detects various forms of malware, generates alerts, and prevents the malware from infecting hosts. Current antivirus products are effective at stopping many instances of malware if their signatures are kept up to date. Antispam software is used to detect spam and prevent it from reaching users’ mailboxes. Spam may contain malware, phishing attacks, and other malicious content, so alerts from antispam software may indicate attack attempts. |
| **File integrity checking software** | File integrity checking software can detect changes made to important files during incidents. It uses a hashing algorithm to obtain a cryptographic checksum for each designated file. If the file is altered and the checksum is recalculated, an extremely high probability exists that the new checksum will not match the old checksum. By regularly recalculating checksums and comparing them with previous values, changes to files can be detected. |
| **Third-party monitoring services** | Third parties offer a variety of subscription-based and free monitoring services. An example is fraud detection services that will notify an organization if its IP addresses, domain names, etc. are associated with current incident activity involving other organizations. There are also free real-time blacklists with similar information. Another example of a third-party monitoring service is a CSIRC notification list; these lists are often available only to other IT Teams. |
| **Logs** | |
| **Operating system, service, and application logs** | Logs from operating systems, services, and applications (particularly audit-related data) are frequently of great value when an incident occurs, such as recording which accounts were accessed and what actions were performed. Organizations should require a baseline level of logging on all systems and a higher baseline level on critical systems. Logs can be used for analysis by correlating event information. Depending on the event information, an alert can be generated to indicate an incident. Section 0 discusses the value of centralized logging. |
| **Network device logs** | Logs from network devices such as firewalls and routers are not typically a primary source of precursors or indicators. Although these devices are usually configured to log blocked connection attempts, they provide little information about the nature of the activity. Still, they can be valuable in identifying network trends and in correlating events detected by other devices. |
| **Network flows** | A network flow is a particular communication session occurring between hosts. Routers and other networking devices can provide network flow information, which can be used to find unusual network activity caused by malware, data exfiltration, and other malicious acts. There are many standards for flow data formats, including NetFlow, sFlow, and IPFIX. |
| **Publicly Available Information** | |
| **Information on new vulnerabilities and exploits** | Keeping up with new vulnerabilities and exploits can prevent some incidents from occurring and assist in detecting and analyzing new attacks. The National Vulnerability Database (NVD) contains information on vulnerabilities.[[10]](#footnote-11) Organizations such as US-CERT[[11]](#footnote-12) and CERT®/CC  periodically provide threat update information through briefings, web postings, and mailing lists. |
| **People** | |
| **People from within the organization** | Users, system administrators, network administrators, and others from within the organization may report signs of incidents. It is important to validate all such reports. One approach is to ask people who provide such information on how confident they are of the accuracy of the information. Recording this estimate, along with the information provided, can help considerably during incident analysis, particularly when conflicting data is discovered. |
| **People from other organizations** | Reports of incidents that originate externally should be taken seriously. For example, the organization might be contacted by a party claiming a system at the organization is attacking its systems. External users may also report other indicators, such as a defaced web page or an unavailable service. Other incident response teams also may report incidents. It is important to have mechanisms in place for external parties to report indicators and for trained staff to monitor those mechanisms carefully; this may be as simple as someone calling the center to report a possible issue. |

Incident Analysis

Incident detection and analysis are not always easily identified. For example, user-provided indicators such as a complaint of a server being unavailable are often incorrect. Intrusion detection systems may produce false positives— incorrect indicators. These examples demonstrate what makes incident detection and analysis difficult: each indicator ideally should be evaluated to determine if it is legitimate. The total number of indicators may be thousands or millions a day. Finding the real security incidents that occurred out of all the indicators can be a daunting task.

Even if an indicator is accurate, it does not necessarily mean that an incident has occurred. Some indicators, such as a server crash or modification of critical files, could happen for several reasons other than a security incident, including human error. Given the occurrence of indicators, however, it is reasonable to suspect that an incident might be occurring and to act accordingly.

Determining whether a particular event is actually an incident is sometimes a matter of judgment. It may be necessary to collaborate with other technical and information security personnel to make a decision. In many instances, a situation should be handled the same way regardless of whether it is security-related. For example, if <<INSERT AGENCY ACRONYM HERE>> is losing Internet connectivity every 12 hours, and no one knows the cause, <<INSERT AGENCY ACRONYM HERE>> would want to resolve the problem just as quickly using the same resources to diagnose the problem, regardless of its cause.

Some incidents are easy to detect, such as an obviously defaced web page. Many incidents are not associated with easily recognized symptoms. Small signs such as one change in one system configuration file may be the only indicators that an incident has occurred. In incident handling, detection may be the most difficult task. There are technical solutions to make detection easier. The best remedy is to build a team of highly experienced and proficient <<INSERT AGENCY ACRONYM HERE>> IT Team. The <<INSERT AGENCY ACRONYM HERE>> IT Team is responsible for analyzing ambiguous, contradictory, and incomplete symptoms to determine what has happened. They can analyze the precursors and indicators effectively and efficiently and take appropriate actions.

The <<INSERT AGENCY ACRONYM HERE>> IT Team should work quickly to analyze and validate each incident, following a pre-defined process and documenting each step taken. When the <<INSERT AGENCY ACRONYM HERE>> IT Team believes that an incident has occurred, <<INSERT AGENCY ACRONYM HERE>> IT Team should rapidly perform an initial analysis to determine the incident’s scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited). The initial analysis should provide enough information for the <<INSERT AGENCY ACRONYM HERE>> IT Team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident.

<<INSERT AGENCY ACRONYM HERE>> has performed the following analysis on its network and shall update as needed:

* **Profile Networks and Systems**. Profiling is measuring the characteristics of expected activity so that changes to it can be more easily identified. Examples of profiling are running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. In practice, it is difficult to detect incidents accurately using most profiling techniques; organizations should use profiling as one of several detection and analysis techniques.
  + <<DESCRIBE WHAT YOURE AGENCY DOES HERE>>
* **Understand Normal Behaviors**. <<INSERT AGENCY ACRONYM HERE>> IT Team members should study networks, systems, and applications to understand what their normal behavior is so that abnormal behavior can be recognized more easily. The <<INSERT AGENCY ACRONYM HERE>> IT Team will not have a comprehensive knowledge of all behavior throughout the environment, but handlers should know which experts could fill in the gaps. One way to gain this knowledge is through reviewing log entries and security alerts. This may be tedious if filtering is not used to condense the logs to a reasonable size. As handlers become more familiar with the logs and alerts, they should be able to focus on unexplained entries, which are usually more important to investigate. Conducting regular log reviews should keep the knowledge fresh, and the analyst should be able to notice trends and changes over time. The reviews also give the analyst an indication of the reliability of each source.
  + <<DESCRIBE WHAT YOURE AGENCY DOES HERE>>
* **Create a Log Retention Policy**. Information regarding an incident may be recorded in several places, such as firewall, IDPS, and application logs. Creating and implementing a log retention policy that specifies how long log data should be maintained may be extremely helpful in analysis because older log entries may show reconnaissance activity or previous instances of similar attacks. Another reason for retaining logs is that incidents may not be discovered until days, weeks, or even months later. The length of time to maintain log data is dependent on several factors, including the organization’s data retention policies and the volume of data. See NIST SP 800-92, Guide to Computer Security Log Management for additional recommendations related to logging[[12]](#footnote-13).
  + <<DESCRIBE WHAT YOURE AGENCY DOES HERE>>
* **Perform Event Correlation**. Evidence of an incident may be captured in several logs that each contain different types of data—a firewall log may have the source IP address that was used. In contrast, an application log may include a username. A network IDPS may detect that an attack was launched against a particular host, but it may not know if the attack was successful. The analyst may need to examine the host’s logs to determine that information. Correlating events among multiple indicator sources can be invaluable in validating whether a particular incident occurred.
  + <<DESCRIBE WHAT YOURE AGENCY DOES HERE>>
* **Keep All Host Clocks Synchronized**. Protocols such as the Network Time Protocol (NTP) synchronize clocks among hosts. Event correlation will be more complicated if the devices reporting events have inconsistent clock settings. From an evidentiary standpoint, it is preferable to have consistent timestamps in logs—for example, to have three logs that show an attack occurred at 12:07:01 a.m., rather than logs that list the attack as occurring at 12:07:01, 12:10:35, and 11:07:06.
  + <<DESCRIBE WHAT YOURE AGENCY DOES HERE>>
* **Maintain and Use a Knowledge Base of Information**. The knowledge base should include information that handlers need for referencing quickly during incident analysis. Although it is possible to build a knowledge base with a complex structure, a simple approach can be effective. Text documents, spreadsheets, and relatively simple databases provide effective, flexible, and searchable mechanisms for sharing data among team members. The knowledge base should also contain a variety of information, including explanations of the significance and validity of precursors and indicators, such as IDPS alerts, operating system log entries, and application error codes.
  + <<DESCRIBE WHAT YOURE AGENCY DOES HERE>>
* **Use Internet Search Engines for Research**. Internet search engines can help analysts find information on unusual activity. For example, an analyst may see some unusual connection attempts targeting TCP port 22912. Performing a search on the terms “TCP,” “port,” and “22912” may return some hits that contain logs of similar activity or even an explanation of the significance of the port number. Note that separate workstations should be used for research to minimize the risk to the organization from conducting these searches.
* **Run Packet Sniffers to Collect Additional Data**. Sometimes the indicators do not record enough detail to permit the handler to understand what is occurring. If an incident is happening over a network, the fastest way to collect the necessary data may be to have a packet sniffer capture network traffic. Configuring the sniffer to record the traffic that matches specified criteria should keep the volume of data manageable and minimize the inadvertent capture of other information. Because of privacy concerns, some organizations may require <<INSERT AGENCY ACRONYM HERE>> IT Teams to request and receive permission before using packet sniffers.
  + <<DESCRIBE WHAT YOURE AGENCY DOES HERE>>
* **Filter the Data**. There is simply not enough time to review and analyze all the indicators; at minimum, the most suspicious activity should be investigated. One effective strategy is to filter out categories of indicators that tend to be insignificant. Another filtering strategy is to show only the categories of indicators that are of the highest significance; however, this approach carries substantial risk because the new malicious activity may not fall into one of the chosen indicator categories.
* **Seek Assistance from Others**. Occasionally, the <<INSERT AGENCY ACRONYM HERE>> IT Team will be unable to determine the full cause and nature of an incident. If <<INSERT AGENCY ACRONYM HERE>> IT Team lacks sufficient information to contain and eradicate the incident, then it should consult with resources such as: Commonwealth Fusion Center, the United States Computer Emergency Response Team (US-CERT), or vendors with incident response expertise. It is important to accurately determine the cause of each incident so that it can be fully contained, and the exploited vulnerabilities can be mitigated to prevent similar incidents from occurring.

Incident Documentation

The <<INSERT AGENCY ACRONYM HERE>> IT Team should immediately start recording all facts regarding the incident.[[13]](#footnote-14) A logbook is an effective and straightforward medium for this,[[14]](#footnote-15). Still, laptops, audio recorders, and digital cameras can also serve this purpose. Documenting system events, conversations, and observed changes in files can lead to a more efficient, more systematic, and less error-prone handling of the problem. Every step taken from the time the incident was detected to its final resolution should be documented and timestamped. Every document regarding the incident should be dated and signed by the <<INSERT AGENCY ACRONYM HERE>> IT Team. Information of this nature can also be used as evidence in a court of law if legal prosecution is pursued. Whenever possible, handlers should work in teams of at least two: one person can record and log events while the other person performs the technical tasks.

IT Team has created <<DESCRIBE WHAT YOURE AGENCY DOES HERE>>.

This log is only available to <<DESCRIBE WHO HAS ACCESS>>.

Incident Prioritization

Prioritizing the handling of the incident is perhaps the most critical decision point in the incident handling process. Incidents should not be handled on a first-come, first-served basis because of resource limitations. Instead, handling should be prioritized based on the relevant factors, such as the following:

* **Functional Impact of the Incident**. Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact on the users of those systems. The <<INSERT AGENCY ACRONYM HERE>> IT Team should consider how the incident will impact the existing functionality of the affected systems. The <<INSERT AGENCY ACRONYM HERE>> IT Team should consider not only the current functional impact of the incident but also the likely future functional impact of the incident if it is not immediately contained.
* **Information Impact of the Incident**. Incidents may affect the confidentiality, integrity, and availability of <<INSERT AGENCY ACRONYM HERE>>’s information. For example, a malicious agent may exfiltrate sensitive information. The <<INSERT AGENCY ACRONYM HERE>> IT Team should consider how this information exfiltration will impact <<INSERT AGENCY ACRONYM HERE>>’s overall mission. An incident that results in the exfiltration of sensitive information may also affect other organizations if any of the data pertains to a partner organization.
* **Recoverability from the Incident**. The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident. In some instances, it is not possible to recover from an incident (e.g., if the confidentiality of sensitive information has been compromised) and it would not make sense to spend limited resources on an elongated incident handling cycle unless that effort was directed at ensuring that a similar incident did not occur in the future. In other cases, an incident may require far more resources to handle than what <<INSERT AGENCY ACRONYM HERE>> has available. The <<INSERT AGENCY ACRONYM HERE>> IT Team should consider the effort necessary to actually recover from an incident and carefully weigh that against the value the recovery effort will create, and any requirements related to incident handling.

Combining the functional impact on <<INSERT AGENCY ACRONYM HERE>>’s systems and the impact on <<INSERT AGENCY ACRONYM HERE>>’s information determines the business impact of the incident. For example, a distributed denial-of-service attack against a public web server may temporarily reduce the functionality for users attempting to access the server. In contrast, unauthorized root-level access to a public webserver may result in the exfiltration of personally identifiable information (PII), which could have a long-lasting impact on <<INSERT AGENCY ACRONYM HERE>>’s reputation.

The recoverability from the incident determines the possible responses that the <<INSERT AGENCY ACRONYM HERE>> IT Team may take when handling the incident. An incident with a high functional impact and low effort to recover from is an ideal candidate for immediate action from the <<INSERT AGENCY ACRONYM HERE>> IT Team. Some incidents may not have smooth recovery paths and may need to be queued for a more strategic-level response—for example, an incident that results in an attacker exfiltrating and publicly posting gigabytes of sensitive data has no easy recovery path since the data is already exposed; in this case, <<INSERT AGENCY ACRONYM HERE>> IT Team may transfer part of the responsibility for handling the data exfiltration incident to a more strategic-level team that develops a strategy for preventing future breaches and creates an outreach plan for alerting those individuals or organizations whose data was exfiltrated. <<INSERT AGENCY ACRONYM HERE>> IT Team should prioritize the response to each incident based on its estimate of the business impact caused by the incident and the estimated efforts required to recover from the incident.

<<INSERT AGENCY ACRONYM HERE>> can best quantify the effect of its incidents because of its situational awareness. The below table provides examples of functional impact categories that an organization might use for rating its incidents. Rating incidents can help prioritize limited resources.

Functional Impact Categories

|  |  |
| --- | --- |
| **Category** | **Definition** |
| None | No effect to the <<INSERT AGENCY ACRONYM HERE>>’s ability to provide all services to all users |
| Low | Minimal effect: <<INSERT AGENCY ACRONYM HERE>> can still provide all critical services to all users but has lost efficiency. Examples include:   * Loss of an email account * Loss of public information * Non-critical files encrypted or deleted * PC becomes corrupted * Non-critical server becomes corrupted but is recoverable |
| Medium | <<INSERT AGENCY ACRONYM HERE>> has lost the ability to provide a critical service to a subset of system users. Examples include:   * Low Impact event impacts multiple users * Reduced functionality for employees * Normal services unavailable, but workarounds are available * Loss of Protected employee data |
| High | <<INSERT AGENCY ACRONYM HERE>> is no longer able to provide some critical services to any users. Examples include:   * Loss of Protected Data * Everything gets encrypted * Data flowing outbound * Loss of functionality |

The below table provides examples of possible information impact categories that describe the extent of information compromise that occurred during the incident. In this table, with the exception of the ‘None’ value, the categories are not mutually exclusive, and the organization could choose more than one.

Information Impact Categories

|  |  |
| --- | --- |
| **Category** | **Definition** |
| None | No information was exfiltrated, changed, deleted, or otherwise compromised |
| Privacy Breach | Sensitive personally identifiable information (PII) of employees or other data like CJIS or Fire/EMS Records. was accessed or exfiltrated |
| Proprietary Breach | Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated |
| Integrity Loss | Sensitive or proprietary information was changed or deleted |

The below table shows examples of recoverability effort categories that reflect the level of, and type of resources required to recover from the incident.

Recoverability Effort Categories

|  |  |
| --- | --- |
| **Category** | **Definition** |
| Regular | Time to recovery is predictable with existing resources |
| Supplemented | Time to recovery is predictable with additional resources |
| Extended | Time to recovery is unpredictable; additional resources and outside help are needed |
| Not Recoverable | Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch an investigation |

Incident Notification

<<DESCRIBE HOW YOUR AGENCY WILL MAKE NOTIFICATIONS OF POTENTIAL INCIDENTS AND TO WHOM>>.

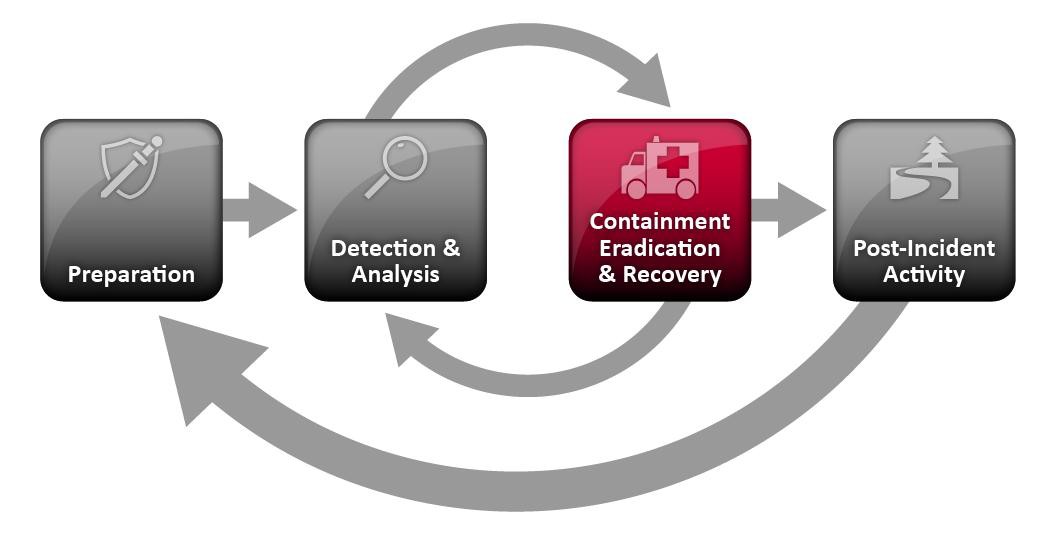
When an incident is analyzed and prioritized, the <<INSERT AGENCY ACRONYM HERE>> IT Team needs to notify the appropriate individuals so that all who need to be involved will play their roles. Incident response policies should include provisions concerning incident reporting—at a minimum, what must be reported to whom and at what times (e.g., initial notification, regular status updates). At <<INSERT AGENCY ACRONYM HERE>>, the following notifications should be made:

|  |  |
| --- | --- |
| Low | * <<LIST WHO TO NOTIFY HERE >> |
| Medium | * <<LIST WHO TO NOTIFY HERE >> |
| High | * <<LIST WHO TO NOTIFY HERE >> |

During incident handling, the <<INSERT AGENCY ACRONYM HERE>> IT Team may need to provide status updates to certain parties, even in some cases the entire organization. <<INSERT AGENCY ACRONYM HERE>> IT Team should plan and prepare several communication methods, including out-of-band methods (e.g., in-person, paper), and select the methods that are appropriate for a particular incident. Possible communication methods include:

* Email;
* Website (internal, external, or portal);
* Telephone calls;
* In-person (e.g., daily briefings);
* Voice mailbox greeting (e.g., set up a separate voice mailbox for incident updates, and update the greeting message to reflect the current incident status; use the help desk’s voice mail greeting); or
* Paper (e.g., post notices on bulletin boards and doors, hand out notices at all entrance points).

Containment, Eradication, and Recovery



Choosing a Containment Strategy

Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident. Containment provides time for developing a tailored remediation strategy. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a network, disable certain functions). Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident; specific strategies are addressed in the IRP on **page C-29.** Containment strategies vary based on the type of incident.

Criteria for determining the appropriate strategy include:

* Potential damage to and theft of resources;
* Need for evidence preservation;
* Service availability (e.g., network connectivity, services provided to external parties);
* Time and resources needed to implement the strategy;
* Effectiveness of the strategy (e.g., partial containment, full containment); and
* Duration of the solution (e.g., an emergency workaround to be removed in four hours, a temporary workaround to be removed in two weeks, permanent solution).

Evidence Gathering and Handling

Although the primary reason for gathering evidence during an incident is to resolve the incident, it may also be needed for legal proceedings.[[15]](#footnote-16) In such cases, it is important to clearly document how all evidence, including compromised systems, has been preserved.[[16]](#footnote-17) Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court.[[17]](#footnote-18) Evidence should be accounted for at all times; whenever evidence is transferred from person to person, a chain of custody forms should detail the transfer and include each party’s signature. A detailed log should be kept for all evidence, including the following:

* Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer)
* Name, title, and phone number of each individual who collected or handled the evidence during the investigation
* Time and date (including time zone) of each occurrence of evidence handling
* Locations where the evidence was stored.

Collecting evidence from computing resources presents some challenges. It is generally desirable to acquire evidence from a system of interest as soon as one suspects that an incident may have occurred. Many incidents cause a dynamic chain of events to occur; an initial system snapshot may do more good in identifying the problem and its source than most other actions that can be taken at this stage. From an evidentiary standpoint, it is much better to get a snapshot of the system as-is rather than doing so after the <<INSERT AGENCY ACRONYM HERE>> IT Team, system administrators, and others have inadvertently altered the state of the machine during the investigation. Users and system administrators should be made aware of the steps that they should take to preserve evidence. See [NIST SP 800-86](https://csrc.nist.gov/publications/detail/sp/800-86/final), Guide to Integrating Forensic Techniques into Incident Response, for additional information on preserving evidence.

Identifying the Attacking Hosts

During incident handling, system owners and others sometimes want to or need to identify the attacking host or hosts. Although this information can be important, the <<INSERT AGENCY ACRONYM HERE>> IT Team should generally stay focused on containment, eradication, and recovery. Identifying an attacking host can be a time-consuming and futile process that can prevent a team from achieving its primary goal—minimizing the business impact. The following items describe the most commonly performed activities for attacking host identification:

* **Validating the Attacking Host’s IP Address**. The <<INSERT AGENCY ACRONYM HERE>> IT Team should focus on the attacking host’s IP address. The handler may attempt to validate that the address was not spoofed by verifying connectivity to it; however, this simply indicates that a host at that address does or does not respond to the requests. A failure to respond does not mean the address is not real—for example, a host may be configured to ignore pings and traceroutes. Also, the attacker may have received a dynamic address that has already been reassigned to someone else.
* **Researching the Attacking Host through Search Engines**. Performing an Internet search using the apparent source IP address of an attack may lead to more information on the attack—for example, a mailing list message regarding a similar attack.
* **Using Incident Databases**. Several groups collect and consolidate incident data from various organizations into incident databases. This information sharing may take place in many forms, such as trackers and real-time blacklists. The organization can also check its own knowledge base or issue tracking system for related activity.
* **Monitoring Possible Attacker Communication Channels**. The <<INSERT AGENCY ACRONYM HERE>> IT Team can monitor communication channels that may be used by an attacking host. For example, many bots use IRC as their primary means of communication. Also, attackers may congregate on certain IRC channels to brag about their compromises and share information. However, the <<INSERT AGENCY ACRONYM HERE>> IT Team should treat any such information that they acquire only as a potential lead, not as fact.

Eradication and Recovery

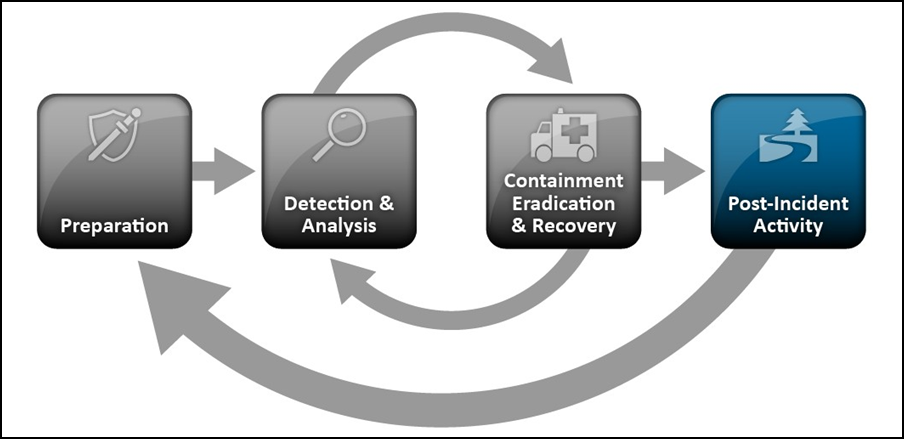
After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts, as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery.

In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists). Higher levels of system logging or network monitoring are often part of the recovery process. Once a resource is successfully attacked, it is often attacked again, or other resources within the organization are attacked in a similar manner.

Eradication and recovery should be done in a phased approach so that remediation steps are prioritized. For large-scale incidents, recovery may take months; the intent of the early phases should be to increase the overall security with relatively quick (days to weeks) high-value changes to prevent future incidents. The later phases should focus on longer-term changes (e.g., infrastructure changes) and ongoing work to keep the enterprise as secure as possible.

Because eradication and recovery actions are typically OS or application-specific, detailed recommendations and advice regarding them are outside the scope of this document.

Post-Incident Activity



After-Action Review

One of the most important parts of incident response is also the most often omitted: learning and improving. Each <<INSERT AGENCY ACRONYM HERE>> IT Team should evolve to reflect new threats, improved technology, and lessons learned. Holding an After-Action Review, or “lessons learned,” meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, can be extremely helpful in improving security measures and the incident handling process itself. Multiple incidents can be covered in a single lessons-learned meeting. This meeting provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident. Questions to be answered in the meeting include:

* Exactly what happened, and at what times?
* How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
* What information was needed sooner?
* Were any steps or actions taken that might have inhibited the recovery?
* What would the staff and management do differently the next time a similar incident occurs?
* How could information sharing with other organizations have been improved?
* What corrective actions can prevent similar incidents in the future?
* What precursors or indicators should be watched for in the future to detect similar incidents?
* What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Small incidents need limited post-incident analysis, with the exception of incidents performed through new attack methods that are of widespread concern and interest. After serious attacks have occurred, it is usually worthwhile to hold post-mortem meetings that cross team and organizational boundaries to provide a mechanism for information sharing. The primary consideration in holding such meetings is ensuring that the right people are involved. Not only is it important to invite people who have been involved in the incident that is being analyzed, but also it is wise to consider who should be invited to facilitate future cooperation.

The success of such meetings also depends on the agenda. Collecting input about expectations and needs (including suggested topics to cover) from participants before the meeting increases the likelihood that the participants’ needs will be met. In addition, establishing rules of order before or during the start of a meeting can minimize confusion and discord. Having one or more moderators who are skilled in group facilitation can yield a high payoff. Finally, it is also important to document the major points of agreement and action items and to communicate them to parties who could not attend the meeting.

Lessons learned meetings provide other benefits. Reports from these meetings are good material for training new team members by showing them how more experienced team members respond to incidents. Updating incident response policies and procedures is another important part of the lessons learned process. Post-mortem analysis of the way an incident was handled will often reveal a missing step or an inaccuracy in a procedure, providing an impetus for change. Because of the changing nature of information technology and changes in personnel, the <<INSERT AGENCY ACRONYM HERE>> IT Team should review all related documentation and procedures for handling incidents at designated intervals.

Another important post-incident activity is creating a follow-up report for each incident, which can be quite valuable for future use. The report provides a reference that can be used to assist in handling similar incidents. Creating a formal chronology of events (including timestamped information such as log data from systems) is important for legal reasons, as is creating a monetary estimate of the amount of damage the incident caused. This estimate may become the basis for subsequent prosecution activity. Follow-up reports should be kept for a period of time as specified in record retention policies.

Using Collected Incident Data

Lessons learned activities should produce a set of objective and subjective data regarding each incident. Over time, the collected incident data should be useful in several capacities. The data, particularly the total hours of involvement and the cost, may be used to justify additional funding of the <<INSERT AGENCY ACRONYM HERE>> IT Team. A study of incident characteristics may indicate systemic security weaknesses and threats, as well as changes in incident trends. This data can be put back into the risk assessment process, ultimately leading to the selection and implementation of additional controls.

Organizations should focus on collecting data that is actionable, rather than collecting data simply because it is available. For example, counting the number of precursor port scans that occur each week and producing a chart at the end of the year that shows port scans increased by eight percent is not very helpful and may be quite time-consuming. Absolute numbers are not informative – understanding how they represent threats to the business processes of the organization is what matters. Organizations should decide what incident data to collect based on reporting requirements and the expected return on investment from the data (e.g., identifying a new threat and mitigating the related vulnerabilities before they can be exploited.) Possible metrics for incident-related data include:

* **Number of Incidents Handled**.[[18]](#footnote-19) Handling more incidents is not necessarily better—for example, the number of incidents handled may decrease because of better network and host security controls, not because of negligence by the <<INSERT AGENCY ACRONYM HERE>> IT Team. The number of incidents handled is best taken as a measure of the relative amount of work that the <<INSERT AGENCY ACRONYM HERE>> IT Team had to perform, not as a measure of the quality of <<INSERT AGENCY ACRONYM HERE>> IT Team unless it is considered in the context of other measures that collectively indicate work quality. It is more effective to produce separate incident counts for each incident category. Subcategories also can be used to provide more information. For example, a growing number of incidents performed by insiders could prompt stronger policy provisions concerning background investigations for personnel and misuse of computing resources and stronger security controls on internal networks (e.g., deploying intrusion detection software to more internal networks and hosts).
  + **Time Per Incident**. For each incident, time can be measured in several ways:
    - The total amount of labor spent working on the incident
    - Elapsed time from the beginning of the incident-to-incident discovery, to the initial impact assessment, and each stage of the incident handling process (e.g., containment, recovery)
    - How long it took the <<INSERT AGENCY ACRONYM HERE>> IT Team to respond to the initial report of the incident
  + **Objective Assessment of Each Incident**. The response to an incident that has been resolved can be analyzed to determine how effective it was. The following are examples of performing an objective assessment of an incident:
    - Reviewing logs, forms, reports, and other incident documentation for adherence to established incident response policies and procedures
    - Identifying which precursors and indicators of the incident were recorded to determine how effectively the incident was logged and identified
    - Determining if the incident caused damage before it was detected
    - Determining if the actual cause of the incident was identified, and identifying the vector of attack, the vulnerabilities exploited, and the characteristics of the targeted or victimized systems, networks, and applications
    - Determining if the incident is a recurrence of a previous incident
    - Calculating the estimated monetary damage from the incident (e.g., information and critical business processes negatively affected by the incident)
    - Measuring the difference between the initial impact assessment and the final impact assessment
    - Identifying which measures, if any, could have prevented the incident.
  + **Subjective Assessment of Each Incident**. <<INSERT AGENCY ACRONYM HERE>> IT Team members may be asked to assess their performance, as well as that of other team members and the entire team. Another valuable source of input is the owner of a resource that was attacked, in order to determine if the owner thinks the incident was handled efficiently and if the outcome was satisfactory.

Besides using these metrics to measure <<INSERT AGENCY ACRONYM HERE>> IT Team’s success, organizations may also find it useful to audit their incident response programs periodically. Audits will identify problems and deficiencies that can then be corrected. At a minimum, an incident response audit should evaluate the following items against applicable regulations, policies, and generally accepted practices:

* Incident response policies, plans, and procedures
* Tools and resources
* Team model and structure
* <<INSERT AGENCY ACRONYM HERE>> IT Team training and education
* Incident documentation and reports
* The measures of success discussed earlier in this section.

Evidence Retention

<<INSERT AGENCY ACRONYM HERE>> complies with all relevant public records laws to retain physical and virtual files.

Coordination and Information Sharing

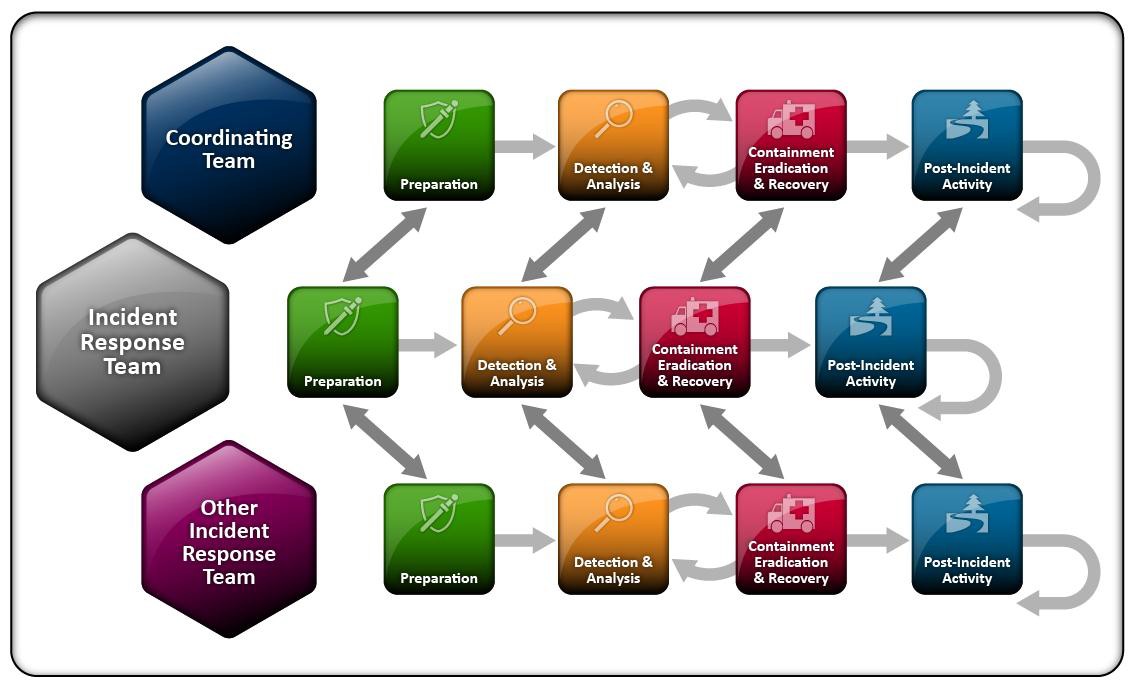
The nature of contemporary threats and attacks makes it more important than ever for organizations to work together during incident response. <<INSERT AGENCY ACRONYM HERE>> should ensure that they effectively coordinate portions of their incident response activities with appropriate partners. The most important aspect of incident response coordination is information sharing, where different organizations share threat, attack, and vulnerability information with each other so that each organization’s knowledge benefits the other. Incident information sharing is frequently mutually beneficial because the same threats and attacks often affect multiple organizations simultaneously.

As mentioned on **page C-4,** coordinating and sharing information with partner organizations can strengthen <<INSERT AGENCY ACRONYM HERE>>’s ability to respond to IT incidents effectively. For example, if <<INSERT AGENCY ACRONYM HERE>> identifies some behavior on its network that seems suspicious and sends information about the event to a set of trusted partners, someone else in that network may have already seen similar behavior and be able to respond with additional details about the suspicious activity, including signatures, other indicators to look for, or suggested remediation actions. Collaboration with the trusted partner can enable <<INSERT AGENCY ACRONYM HERE>>, and other organizations, to respond to the incident more quickly and efficiently than if it were operating in isolation.

This increase in efficiency for standard incident response techniques is not the only incentive for cross-organization coordination and information sharing. Another incentive for information sharing is the ability to respond to incidents using techniques that may not be available to a single organization, especially if that organization is small to medium size. For example, a small organization that identifies a particularly complex instance of malware on its network may not have the in-house resources to thoroughly analyze the malware and determine its effect on the system. In this case, the organization may be able to leverage a trusted information-sharing network to effectively outsource the analysis of this malware to third-party resources that have adequate technical capabilities to perform the malware analysis.

Coordination

<<INSERT AGENCY ACRONYM HERE>> may need to interact with several types of external organizations in the course of conducting incident response activities. Examples of these organizations include other IT Teams, law enforcement agencies, Internet service providers, and constituents and customers. As such, the <<INSERT AGENCY ACRONYM HERE>> IT Team should plan its incident coordination with those parties before incidents occur to ensure that all parties know their roles and that effective lines of communication are established. The figure below provides a sample view of an organization performing coordination at every phase of the incident response lifecycle, highlighting that coordination is valuable throughout the lifecycle.



Sharing Agreements and Reporting Requirements

Before sharing any information, <<INSERT AGENCY ACRONYM HERE>> should consult with its legal department before initiating any coordination efforts. There may be contracts or other agreements that need to be put into place before discussions occur. An example is a nondisclosure agreement (NDA) to protect the confidentiality of the organization’s most sensitive information. <<INSERT AGENCY ACRONYM HERE>> should also consider any existing requirements for reporting, such as sharing incident information with an ISAC or reporting incidents to a higher-level CIRT.

Information Sharing Techniques

Information sharing is a key element of enabling coordination across organizations. <<INSERT AGENCY ACRONYM HERE>> should perform such information sharing throughout the incident response life cycle and not wait until an incident has been fully resolved before sharing details of it with others.

Incident Response Partners (Vendors, State, Federal)

Vendors

**Vendor Incident Response Partner(s)**

|  |  |
| --- | --- |
| **Organization** | **URL** |
|  |  |

State

**State Incident Response Partners**

|  |  |
| --- | --- |
| **Organization** | **URL or Contact Number** |
| Commonwealth of Massachusetts – Fusion Center | 978-451-3700 |
| EOTSS | <https://www.mass.gov/servicenow> |
| Attorney General’s Cyber Crimes Division | <https://www.mass.gov/the-attorney-generals-cyber-crimes-division> |

Federal

**Federal Incident Response Partners**

|  |  |
| --- | --- |
| **Organization** | **URL** |
| Anti-Phishing Working Group (APWG) | <http://www.antiphishing.org/> |
| Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice | <http://www.cybercrime.gov/> |
| CERT**®** Coordination Center, Carnegie Mellon University (CERT**®**/CC) | <http://www.cert.org/> |
| European Network and Information Security Agency (ENISA) | <http://www.enisa.europa.eu/activities/cert> |
| Forum of Incident Response and Security Teams (FIRST) | <http://www.first.org/> |

Plan Maintenance & Testing

Plan Maintenance

Given that technology continually evolves, this plan shall be reviewed at least once per year. During the review, all procedures should be verified to ensure that they still meet industry standards and best practices. Further, as technology is either commissioned or decommissioned, this plan should be evaluated and edited as needed.

Testing

Testing demonstrates the correct operation of all equipment, procedures, processes, and systems that support <<INSERT AGENCY ACRONYM HERE>>’s computer security incident handling program and ensures that resources and procedures are kept in a constant state of readiness. <<INSERT AGENCY ACRONYM HERE>> will test the following:

* **Annually**
  + User awareness and training
  + Port, Password, and Patch Vulnerability Testing
  + Any other applicable testing based on current threats.
* **Quarterly**
  + Phishing / Spear-phishing test
  + Any other applicable testing based on current threats.

Cyber Incident Response Plan

Overview

Incident handling scenarios provide an inexpensive and effective way to build incident response skills and identify potential issues with incident response processes. The <<INSERT AGENCY ACRONYM HERE>> IT Team or team members are presented with a scenario and a list of related questions. <<INSERT AGENCY ACRONYM HERE>> IT Team then discusses each question and determines the most likely answer. The goal is to determine what <<INSERT AGENCY ACRONYM HERE>> IT Team would do and to compare that with policies, procedures, and generally recommended practices to identify discrepancies or deficiencies. For example, the answer to one question may indicate that the response would be delayed because <<INSERT AGENCY ACRONYM HERE>> IT Team lacks a piece of software or because another team does not provide off-hours support. The questions listed below apply to almost any scenario. Each question is followed by a reference to the related section(s) of the document.

Questions to Consider

**Preparation:**

* + - * Would <<INSERT AGENCY ACRONYM HERE>> consider this activity to be an incident? If so, which policies does this activity violate?
      * What measures are in place to attempt to prevent this type of incident from occurring or to limit its impact?

**Detection and Analysis:**

* + - * What precursors of the incident, if any, might <<INSERT AGENCY ACRONYM HERE>> detect? Would any precursors cause us to take action before the incident occurred?
      * What indicators of the incident might <<INSERT AGENCY ACRONYM HERE>> detect? Which indicators would cause someone to think that an incident might have occurred?
      * What additional tools might be needed to detect this particular incident?
      * How would the <<INSERT AGENCY ACRONYM HERE>> IT Team analyze and validate this incident? What personnel would be involved in the analysis and validation process?
      * Who should the <<INSERT AGENCY ACRONYM HERE>> on-duty supervisor notify regarding a suspected incident?
      * How would the <<INSERT AGENCY ACRONYM HERE>> IT Team prioritize the handling of this incident?

**Containment, Eradication, and Recovery:**

* + - * What strategy should <<INSERT AGENCY ACRONYM HERE>> take to contain the incident? Why is this strategy preferable to others?
      * What could happen if the incident were not contained?
      * What additional tools might be needed to respond to this particular incident?
      * Which personnel would be involved in the containment, eradication, and/or recovery processes?
      * What sources of evidence, if any, should we acquire? How would the evidence be acquired? Where would it be stored? How long should it be retained?

**Post-Incident Activity:**

* + - * Who should attend the lessons learned meeting regarding this incident?
      * What should be done to prevent similar incidents from occurring in the future?
      * What should be done to improve the detection of similar incidents?

**General Questions:**

* + - * How many <<INSERT AGENCY ACRONYM HERE>> IT Team members would participate in handling this incident?
      * Besides the <<INSERT AGENCY ACRONYM HERE>> IT Team, who else within the organization should be involved in handling this incident?
      * To which external parties would <<INSERT AGENCY ACRONYM HERE>> IT Team report the incident? When would each report occur? How would each report be made? What information would you report or not report, and why?
      * What other communications with external parties may occur?
      * What tools and resources would <<INSERT AGENCY ACRONYM HERE>> IT Team use in handling this incident?
      * What aspects of the handling would have been different if the incident had occurred on a different day and time (Administrative on-hours versus off-hours)?
      * What aspects of the handling would have been different if the incident had occurred at a different physical location (onsite versus offsite)?

Active Incident Considerations

* What was compromised?
  + Notify <<SECURITY VENDOR>>
  + Search the network
  + Damage assessment –
    - determine what was lost
    - which computers/servers were affected?
    - Determine the level of severity
* All employees change passwords.
* Log into each machine
* Network/Virus scans on all systems
  + Create a data recovery process
* Perform After-Action Review

1. Reporting Incidents

Cyber incidents can have serious consequences. The theft of private, or other sensitive data, and cyber incidents that damage computer systems are capable of causing lasting harm to <<INSERT AGENCY ACRONYM HERE>>, its member communities, and all other users of the Internet.

In addition to law enforcement, other responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the State and Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. This Appendix explains when, what, and how, to report a cyber incident.

**When to Report**

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern.

Accordingly, victims are encouraged to report all cyber incidents that may:

* Result in a substantial loss of data, system availability, or control of systems;
* Impact a large number of victims;
* Indicate unauthorized access to, or malicious software present on, critical information technology systems;
* Affect critical infrastructure or core government functions; or
* Impact national security, economic security, or public health and safety.

**What to Report**

A cyber incident may be reported at various stages, even when complete information is not available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

**How to Report Cyber**

<<INSERT AGENCY ACRONYM HERE>> should consider reporting a cyber-incident using Table 1 below. The agency receiving the initial report will coordinate with other relevant stakeholders to respond to the incident.

**Types of Incident Response**

After submitting a report, <<INSERT AGENCY ACRONYM HERE>> may receive assistance with a specific focus on two activities – threat response and asset response.

* Threat response includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter malicious cyber activity.
* Asset response includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to systems and/or data, strengthening, recovering, and restoring services, identifying other entities at risk, and assessing the potential risk to the broader community, and mitigating potential privacy risks to affected individuals.

**Table 1: Key Points of Contact**

|  |  |
| --- | --- |
| **Threat Response** | **Asset Response** |
| **Commonwealth Fusion Center:** 978-451-3700   * Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity. | |
| **Federal Bureau of Investigation (FBI):**  FBI Field Office Cyber Task Forces: [http://www.fbi.gov/contact-](http://www.fbi.gov/contact-us/field) [us/field](http://www.fbi.gov/contact-us/field) | **National Cybersecurity and Communications Integration Center (**[**NCCIC**](http://www.dhs.gov/about-national-cybersecurity-communications-integration-center)**)**  (888) 282-0870 or  [NCCIC@hq.dhs.gov](mailto:NCCIC@hq.dhs.gov) |
| Internet Crime Complaint Center (IC3): [http://www.ic3.gov](http://www.ic3.gov/) |
| * Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces. * Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties. |
| **United States Computer Emergency Readiness Team:**  [http://www.us-cert.gov](http://www.us-cert.gov/)   * Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to improve security further. |
| **National Cyber Investigative Joint Task Force (NCIJTF)**  CyWatch 24/7 Command Center: [cywatch@ic.fbi.gov](mailto:cywatch@ic.fbi.gov) or (855) 292-3937  Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government. |
| **United States Secret Service (USSS)**  Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs): [http://www.secretservice.gov/contact/field-offices](http://www.secretservice.gov/contact/field-offices/)   * Report cybercrime, including computer intrusions or attacks, the transmission of malicious code, password trafficking, or theft of payment card or other financial payment information. |
| **United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI)**  HSI Tip Line: 866-DHS-2-ICE (866-347-2423) or  [www.ice.gov/webform/hsi-tip-form](http://www.ice.gov/webform/hsi-tip-form)  HSI Field Offices: <https://www.ice.gov/contact/hsi>  HSI Cyber Crimes Center: [https://www.ice.gov/cyber-crimes](https://www.ice.gov/cyber-crimes/)  Report a cyber-enabled crime, including digital theft of intellectual property, illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering. |

1. Roles of State/Federal Cybersecurity Centers

The **Federal Government** has established a number of cybersecurity centers associated with various departments and agencies to execute operational missions, enhance information sharing, maintain situational awareness of cyber incidents, and serve as conduits between public- and private-sector stakeholder entities. In support of the Federal Government’s coordinating structures on cyber incident management, a Cyber Unified Coordination Group41 may elect to leverage these cybersecurity centers for their established enhanced coordination procedures, above-steady-state capacity, and/or operational or support personnel.

**National Cybersecurity and Communications Integration Center (NCCIC)**

As an operational element of the Department of Homeland Security, the NCCIC is the primary platform to coordinate the Federal Government’s asset response to cyber incidents. The NCCIC is authorized under Section 3 of the National Cybersecurity Protection Act of 2014.

**National Cyber Investigative Joint Task Force (NCIJTF)**

The NCIJTF is a multi-agency center hosted by the Federal Bureau of Investigation and is the primary platform to coordinate the Federal Government’s threat response. The NCIJTF is chartered under paragraph 31 of National Security Presidential Directive-54/Homeland Security Presidential Directive-23.

C**yber Threat Intelligence Integration Center (CTIIC)**

Operated by the Office of the Director of National Intelligence, the CTIIC is the primary platform for intelligence integration, analysis, and supporting activities for the Federal Government. CTIIC also provides an integrated all-source analysis of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests.

**U.S. Cyber Command (USCYBERCOM) Joint Operations Center (JOC)**

The USCYBERCOM JOC directs the U.S. military’s cyberspace operations and defense of the Department of Defense Information Network (DoDIN). USCYBERCOM manages both the threat and asset responses for the DoDIN during incidents affecting the DoDIN and receives support from the other centers, as needed.

**National Security Agency Cybersecurity Threat Operations Center (NCTOC)**

The National Security Agency Cybersecurity Threat Operations Center (NCTOC) is the 24/7/365 NSA element that characterizes and assesses foreign cybersecurity threats. The NCTOC informs partners of current and potential malicious cyber activity through its analysis of foreign intelligence, with a focus on adversary computer network attacks, capabilities, and exploitations. Upon request, the NCTOC also provides technical assistance to U.S. Government departments and agencies.

**Intelligence Community – Security Coordination Center (IC-SCC)**

The IC-SCC mission is to monitor and oversee the integrated defense of the IC Information Environment in conjunction with IC mission partners and in accordance with the authority and direction of the Office of the Director of National Intelligence Chief Information Officer. The IC - Incident Response Center roles and responsibilities were assumed upon the IC SCC’s founding in 2014.

1. Core Capabilities and Critical Tasks

Each core capability identified in the Cyber Incident Response Plan (CIRP) has critical tasks that facilitate capability execution. These critical tasks are tasks that are essential to achieving the desired outcome of the capability. Critical tasks inform mission objectives, which allow planners to identify resourcing and sourcing requirements prior to an incident. The chart below describes each core capability and identifies critical tasks associated with each capability.

|  |
| --- |
| **Core Capabilities and Critical Tasks** |
| **1. Access Control and Identity Verification**  **Description:** Apply and support necessary physical, technological, and cyber measures to control admittance to critical locations and systems. Also referred to as Authentication and Authorization. |
| **Critical Tasks:**   * Verify identity to authorize, grant, or deny access to cyber assets, networks, applications, and systems that could be exploited to do harm. * Control and limit access to critical locations and systems to authorized individuals carrying out legitimate activities. * Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. * Perform audit activities to verify and validate security mechanisms that are performing as intended. * Conduct training to ensure staff-wide adherence to access control authorizations. |
| **2. Cybersecurity**  **Description:** Protect (and, if needed, restore) computer networks, electronic communications systems, information, and services from damage, unauthorized use, and exploitation. More commonly referred to as computer network defense, these activities ensure the security, reliability, confidentiality, integrity, and availability of critical information, records, and communications systems and services through collaborative initiatives and efforts. |
| **Critical Tasks:**   * Implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that could be exploited. * Secure, to the extent possible, public, and private networks and critical infrastructure (e.g., communication, financial, electricity sub-sector, water, and transportation systems), based on vulnerability results from risk assessment, mitigation, and incident response capabilities. * Create resilient cyber systems that allow for the uninterrupted continuation of essential functions. * Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. * Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners. |

|  |
| --- |
| **Core Capabilities and Critical Tasks** |
| **3. Forensics and Attribution**  **Description:** Forensic investigations and efforts to provide attribution for an incident are complementary functions that often occur in parallel during a significant cyber incident. |
| **Critical Tasks:**   * Retrieve digital media and data network security and activity logs. * Conduct digital evidence analysis and respecting the chain of custody rules. * Conduct physical evidence collections; analysis adheres to rules of evidence collection as necessary. * Assess the capabilities of likely threat actors(s). * Leverage the work of incident responders and technical attribution assets to identify the malicious cyber actor(s). * Interview witnesses, potential associates, and/or perpetrators if possible. * Apply confidence levels to attribution assignments. * Include suitable inclusion and limitation information for sharing products in attribution elements guidance. * Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. * Perform audit activities to verify and validate security mechanisms that are performed as intended. |
| **4. Infrastructure Systems**  **Description:** Stabilize critical infrastructure functions, minimize health and safety threats, and efficiently respond and recover systems and services to support a viable, resilient community following malicious cyber activity. |
| **Critical Tasks:**   * Maintain a comprehensive understanding of the needs for the safe operation of control systems. * Stabilize and regain control of infrastructure. * Increase network isolation to reduce the risk of a malicious cyber activity propagating more widely across the enterprise or among interconnected entities. * Stabilize infrastructure within those entities that may be affected by the cascading effects of the cyber incident. * Facilitate the restoration and sustainment of essential services (public and private) to maintain community functionality. * Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. * Maintain up-to-date data knowledge of applicable emerging and existing security research, development, and solutions. |

|  |
| --- |
| **Core Capabilities and Critical Tasks** |
| **5. Intelligence and Information Sharing**  **Description:** Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning threats of malicious cyber activity to the United States, its people, property, or interests. Intelligence and information sharing are the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as necessary. |
| **Critical Tasks:**   * Monitor, analyze, and assess the positive and negative impacts of changes in the operating environment as it pertains to cyber vulnerabilities and threats. * Share analysis results through participation in the routine exchange of security information— including threat assessments, alerts, threat indications and warnings, and advisories—among partners. * Confirm intelligence and information sharing requirements for cybersecurity stakeholders. * Develop or identify and provide access to mechanisms and procedures for confidential intelligence and information sharing between the private sector and government cybersecurity partners.[42](#_bookmark97) * Use intelligence processes to produce and deliver relevant, timely, accessible, and actionable intelligence and information products to others as applicable, to include critical infrastructure participants and partners with roles in physical response efforts. * Share actionable cyber threat information with SLTT and international governments and private sectors to promote shared situational awareness. * Enable collaboration via online networks that are accessible to all participants. * Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. |

42 Information sharing must provide effective communication to individuals with access and functional needs, including people with limited English proficiency and people with disabilities, including people who are deaf or hard of hearing and people who are blind or have low vision. Effective communication with individuals with access and functional needs includes the use of appropriate auxiliary aids and services, such as sign language and other interpreters, captioning of audio and video materials, user-accessible Web sites, communication in various languages, and use of culturally diverse media outlets.

|  |
| --- |
| **Core Capabilities and Critical Tasks** |
| **6. Interdiction and Disruption**  **Description:** Delay, divert, intercept, halt, apprehend, or secure threats related to the malicious cyber activity. |
| **Critical Tasks:**   * Deter malicious cyber activity within the United States, its territories, and abroad. * Interdict persons associated with a potential cyber threat or act. * Deploy assets to interdict, deter, or disrupt cyber threats from reaching the potential target(s). * Leverage law enforcement and intelligence assets to identify, track, investigate, and disrupt malicious actors threatening the security of the Nation’s public and private information systems. * Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. * Respect defined limitations and frontiers of cybersecurity policy among collaborative security partners. |
| **7. Logistics and Supply Chain Management**  **Description:** Facilitate and assist with the delivery of essential commodities, equipment, and services to include the sustainment of responders in support of responses to systems and networks impacted by malicious cyber activity. Synchronize logistics capabilities and enable the restoration of impacted supply chains. |
| **Critical Tasks:**   * Identify and catalog resources needed for response, prior to mobilization. * Mobilize and deliver governmental, nongovernmental, and private sector resources to stabilize the incident and integrate response and recovery efforts, to include moving and delivering resources and services to meet the needs of those impacted by a cyber incident. * Facilitate and assist the delivery of critical infrastructure components to rapid response and restoration of cyber systems. * Enhance public and private resource and services support for impacted critical infrastructure entities. * Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information and protecting individual privacy, civil rights, and civil liberties. * Apply supply chain assurance principles and knowledge within all critical tasks identified above. |

1. Additional Resources

The lists below provide examples of resources that may help establish and maintain an incident response capability.

**Incident Response Organizations**

|  |  |
| --- | --- |
| **Organization** | **URL** |
| Anti-Phishing Working Group (APWG) | <http://www.antiphishing.org/> |
| Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice | <http://www.cybercrime.gov/> |
| CERT**®** Coordination Center, Carnegie Mellon University (CERT**®**/CC) | <http://www.cert.org/> |
| European Network and Information Security Agency (ENISA) | <http://www.enisa.europa.eu/activities/cert> |
| Forum of Incident Response and Security Teams (FIRST) | <http://www.first.org/> |
| Government Forum of Incident Response and Security Teams (GFIRST) | <http://www.us-cert.gov/federal/gfirst.html> |
| High Technology Crime Investigation Association (HTCIA) | <http://www.htcia.org/> |
| InfraGard | <http://www.infragard.net/> |
| Internet Storm Center (ISC) | <http://isc.sans.edu/> |
| National Council of ISACs | <http://www.isaccouncil.org/> |
| United States Computer Emergency Response Team (US-CERT) | <http://www.us-cert.gov/> |

**NIST Publications**

|  |  |
| --- | --- |
| **Resource Name** | **URL** |
| NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* | <http://csrc.nist.gov/publications/PubsSPs.html#800-53> |
| NIST SP 800-83, *Guide to Malware Incident Prevention and Handling* | <http://csrc.nist.gov/publications/PubsSPs.html#800-83> |
| NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* | <http://csrc.nist.gov/publications/PubsSPs.html#800-84> |
| NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response* | <http://csrc.nist.gov/publications/PubsSPs.html#800-86> |
| NIST SP 800-92, *Guide to Computer Security Log Management* | <http://csrc.nist.gov/publications/PubsSPs.html#800-92> |
| NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)* | <http://csrc.nist.gov/publications/PubsSPs.html#800-94> |
| NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* | <http://csrc.nist.gov/publications/PubsSPs.html#800-115> |
| NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems* | <http://csrc.nist.gov/publications/PubsSPs.html#800-128> |
|  |  |

**Data Exchange Specifications Applicable to Incident Handling**

|  |  |  |
| --- | --- | --- |
| **Title** | **Description** | **Additional Information** |
| AI | Asset Identification | <http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-> [IR-7693](http://csrc.nist.gov/publications/PubsNISTIRs.html%23NIST-IR-7693) |
| ARF | Asset Results Format | <http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-> [IR-7694](http://csrc.nist.gov/publications/PubsNISTIRs.html%23NIST-IR-7694) |
| CAPEC | Common Attack Pattern Enumeration and Classification | <http://capec.mitre.org/> |
| CCE | Common Configuration Enumeration | <http://cce.mitre.org/> |
| CEE | Common Event Expression | <http://cee.mitre.org/> |
| CPE | Common Platform Enumeration | <http://cpe.mitre.org/> |
| CVE | Common Vulnerabilities and Exposures | <http://cve.mitre.org/> |
| CVSS | Common Vulnerability Scoring System | <http://www.first.org/cvss/cvss-guide> |
| CWE | Common Weakness Enumeration | <http://cwe.mitre.org/> |
| CybOX | Cyber Observable eXpression | <http://cybox.mitre.org/> |
| MAEC | Malware Attribute Enumeration and Characterization | <http://maec.mitre.org/> |
| OCIL | Open Checklist Interactive Language | <http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-> [IR-7692](http://csrc.nist.gov/publications/PubsNISTIRs.html%23NIST-IR-7692) |
| OVAL | Open Vulnerability Assessment Language | <http://oval.mitre.org/> |
| RFC 4765 | Intrusion Detection Message Exchange Format (IDMEF) | <http://www.ietf.org/rfc/rfc4765.txt> |
| RFC 5070 | Incident Object Description Exchange Format (IODEF) | <http://www.ietf.org/rfc/rfc5070.txt> |
| RFC 5901 | Extensions to the IODEF for Reporting Phishing | <http://www.ietf.org/rfc/rfc5901.txt> |
| RFC 5941 | Sharing Transaction Fraud Data | <http://www.ietf.org/rfc/rfc5941.txt> |
| RFC 6545 | Real-time Inter-network Defense (RID) | <http://www.ietf.org/rfc/rfc6545.txt> |
| RFC 6546 | Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS | <http://www.ietf.org/rfc/rfc6546.txt> |
| SCAP | Security Content Automation Protocol | [http://csrc.nist.gov/publications/PubsSPs.html #SP-800-](http://csrc.nist.gov/publications/PubsSPs.html%23SP-800-126-Rev.%202) [126-Rev.%202](http://csrc.nist.gov/publications/PubsSPs.html%23SP-800-126-Rev.%202) |
| XCCDF | Extensible Configuration Checklist Description Format | <http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-> [IR-7275-r4](http://csrc.nist.gov/publications/PubsNISTIRs.html%23NIST-IR-7275-r4) |

1. Acronyms

Selected acronyms used in the publication are defined below.

**CCIPS** Computer Crime and Intellectual Property Section

**CERIAS** Center for Education and Research in Information Assurance and Security

**CERT®/CC** CERT**®** Coordination Center

**CIO** Chief Information Officer

**CIRC** Computer Incident Response Capability

**CIRC** Computer Incident Response Center

**CIRT** Computer Incident Response Team

**CISO** Chief Information Security Officer

**CSIRC** Computer Security Incident Response Capability

**CSIRT** Computer Security Incident Response Team

**DDoS** Distributed Denial of Service

**DHS** Department of Homeland Security

**DNS** Domain Name System

**DoS** Denial of Service

**FAQ** Frequently Asked Questions

**FBI** Federal Bureau of Investigation

**FIPS** Federal Information Processing Standards

**FIRST** Forum of Incident Response and Security Teams

**FISMA** Federal Information Security Management Act

**GAO** General Accountability Office

**GFIRST** Government Forum of Incident Response and Security Teams

**GRS** General Records Schedule

**HTTP** HyperText Transfer Protocol

**IANA** Internet Assigned Numbers Authority

**IDPS** Intrusion Detection and Prevention System

**IETF** Internet Engineering Task Force

**IP** Internet Protocol

**IR** Interagency Report

**IRC** Internet Relay Chat

**ISAC** Information Sharing and Analysis Center

**ISP** Internet Service Provider

**IT** Information Technology

**ITL** Information Technology Laboratory

**MAC** Media Access Control

**MOU** Memorandum of Understanding

**MSSP** Managed Security Services Provider

**NAT** Network Address Translation

**NDA** Non-Disclosure Agreement

**NIST** National Institute of Standards and Technology

**NSRL** National Software Reference Library

**NTP** Network Time Protocol

**NVD** National Vulnerability Database

**OIG** Office of Inspector General

**OMB** Office of Management and Budget

**OS** Operating System

**PII** Personally Identifiable Information

**PIN** Personal Identification Number

**POC** Point of Contact

**REN-ISAC** Research and Education Networking Information Sharing and Analysis Center

**RFC** Request for Comment

**RID** Real-Time Inter-Network Defense

**SIEM** Security Information and Event Management

**SLA** Service Level Agreement

**SOP** Standard Operating Procedure

**SP** Special Publication

**TCP** Transmission Control Protocol

**TCP/IP** Transmission Control Protocol/Internet Protocol

**TERENA** Trans-European Research and Education Networking Association

**UDP** User Datagram Protocol

**URL** Uniform Resource Locator

**US-CERT** United States Computer Emergency Readiness Team

**VPN** Virtual Private Network

1. Incident Handling Checklist

This checklist provides the major steps to be performed in the handling of an incident. Note that the actual steps performed may vary based on the type of incident and the nature of individual incidents. For example, if the handler knows precisely what has happened based on an analysis of indicators (Step 1.2), there may be no need to perform Steps 1.3 or 1.4 to research the activity further. The checklist provides guidelines to handlers on the major steps that should be performed; it does not dictate the exact sequence of steps that should always be followed.

|  |  |  |
| --- | --- | --- |
|  | **Action** | **Completed** |
| **Detection and Analysis** | | |
| 1. | Determine whether an incident has occurred |  |
| 1.1 | <<INSERT AGENCY ACRONYM HERE>> Supervisor makes notification according to Section 0 |  |
| 1.2 | Analyze the precursors and indicators |  |
| 1.3 | Look for correlating information |  |
| 1.4 | Perform research (e.g., search engines, knowledge base) |  |
| 1.5 | As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence |  |
| 2. | Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.) |  |
| 3. | Report the incident to the appropriate internal personnel and external organizations |  |
| **Containment, Eradication, and Recovery** | | |
| 4. | Acquire, preserve, secure, and document evidence |  |
| 5. | Contain the incident |  |
| 6. | Eradicate the incident |  |
| 6.1 | Identify and mitigate all vulnerabilities that were exploited |  |
| 6.2 | Remove malware, inappropriate materials, and other components |  |
| 6.3 | If more affected hosts are discovered (e.g., new malware infections), repeat  the Detection and Analysis steps to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them |  |
| 7. | Recover from the incident |  |
| 7.1 | Return affected systems to an operationally ready state |  |
| 7.2 | Confirm that the affected systems are functioning normally |  |
| 7.3 | If necessary, implement additional monitoring to look for future related activity |  |
| **Post-Incident Activity** | | |
| 8. | Create a follow-up report |  |
| 9. | Hold a lessons-learned meeting (mandatory for major incidents, optional otherwise) |  |

1. Annex – Public Health Emergency

The following section contains the <<INSERT AGENCY ACRONYM HERE>> Public Health Emergency Plan.

Public Health Emergencies will vary from one situation to another. A localized Emerging Infectious Disease may be isolated to one community or one event. Whereas a pandemic would be widespread in multiple countries with localized community spread.

This section has been developed to aid in pandemic planning. Since a pandemic would likely be dealing with an emerging infectious disease, the below guide should be used in consideration of the current recommendations by the World Health Organization (WHO), the Center for Disease Control and Prevention (CDC), the Massachusetts Department of Health & Human Services, and local municipal boards of health.

**Social Distancing Considerations**

* Limit access to employees and essential traffic
* If possible separate telecommunicators to allow 6 feet between them
* Stop physical console changes during shift – instead, this can be done virtually
* Limit training rooms and conference rooms to only <<INSERT AGENCY ACRONYM HERE>> personnel
* Avoid in-person meetings unless essential – instead, use other methods such as webinars/Teams/ Zoom/ GoToMeeting
* Suspend work-related travel
* Suspend employee personal travel and/or institute self-isolation guidelines upon return Policy
* Review COOPs/Contingency Plans and make situational adjustments as needed to include decontamination of the PSAP if it becomes necessary
* Activate Contingency Staffing Plans
* Test all backup equipment and sites
* Activate disaster security protocols for primary and backup sites
* Make changes to policy/procedure/protocols as needed – policy/procedure changes may come from responder partners and protocol changes may come from the dispatch protocol vendor
* Assign someone to monitor the protocol vendor website to keep up with changes
* Review all internal and external resource contact numbers to make sure they are current – such as response partners, public support agencies
* Ascertain if any changes can be made to lighten the non-emergency load on telecommunicators – could be an alternate center/EOC be activated, redirect of some or all non-emergency calls

**Employee Health Considerations**

* Create or adopt health attestation form for essential visitors
* Use ≥ 60% hand sanitizer and deploy it at strategic points in the center (preferably at each console and in each office)
* Implement health screenings for employees reporting to work
* Record temperature checks prior to entering the building – create a baseline based on CDC guidance and do not waiver from it
* Frequently wash your hands using soap and water for at least 20 seconds
* Notice to employees advising ways to stay healthy:
  + Employees should self-monitor and watch for signs and symptoms of the virus
  + Employees who are demonstrating symptoms or feel ill will notify their supervisor, describe their symptoms, and not report to work
  + Employees who have a household member or close contact who has been diagnosed or is symptomatic will notify their supervisor and should not report to duty
  + Employees should not return to work until fully recovered from the virus and be free of symptoms for 72 hours, or on the clearance of a healthcare provider or the local health department
  + Avoid touching face, eyes, nose, mouth, and any other mucous membranes
  + Practice respiratory etiquette by covering coughs and sneezes
  + Promptly dispose of used tissues in a trash receptacle
* Consider limiting employees to pick up food while on duty
* Identify available CISM support, establish a check-in schedule with CISM resources
* Monitor staff physical and mental health as the event unfolds Public Information
* Create a contact schedule or recurring conference call with response partners to keep informed of changing policies, procedures, protocols, or plans. Or, as an alternate, issue Situation Reports (SitReps) to member agencies with the same message.
* Create media messages including social media messages to assist the public accessing assistance and information – include any agency services that have been suspended

Cleaning & Supplies

* Contract with industrial cleaning agency for deep cleaning should it become necessary
* Increase the frequency of existing janitorial services
* Disinfect surfaces at every shift change if possible, but at least twice a day
* Ensure adequate cleaning supplies are on hand
* Supplies for extended shifts
* Consider ordering supplies like gloves or masks.

1. The National Software Reference Library (NSRL) Project maintains records of hashes of various files, including operating system, application, and graphic image files. The hashes can be downloaded from <http://www.nsrl.nist.gov/>. [↑](#footnote-ref-2)
2. Guidelines on risk assessment are available in NIST SP 800-30, Guide for Conducting Risk Assessments, at <http://csrc.nist.gov/publications/PubsSPs.html#800-30-Rev1> [↑](#footnote-ref-3)
3. Information on identifying critical resources is discussed in FIPS 199, Standards for Security Categorization of Federal

   Information and Information Systems, at <http://csrc.nist.gov/publications/PubsFIPS.html> [↑](#footnote-ref-4)
4. For more information on continuous monitoring, see NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations (<http://csrc.nist.gov/publications/PubsSPs.html#800-137>) [↑](#footnote-ref-5)
5. More information on SCAP is available from NIST SP 800-117 Revision 1, Guide to Adopting and Using the Security

   Content Automation Protocol (SCAP) Version 1.2 (<http://csrc.nist.gov/publications/PubsSPs.html#800-117>). [↑](#footnote-ref-6)
6. NIST hosts a security checklists repository at <http://checklists.nist.gov/>. [↑](#footnote-ref-7)
7. More information on malware prevention is available from NIST SP 800-83, Guide to Malware Incident Prevention and Handling (<http://csrc.nist.gov/publications/PubsSPs.html#800-83>). [↑](#footnote-ref-8)
8. Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities,

   <http://csrc.nist.gov/publications/PubsSPs.html#800-84> [↑](#footnote-ref-9)
9. See NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems, for additional information on IDPS products. It is available at <http://csrc.nist.gov/publications/PubsSPs.html#800-94>. [↑](#footnote-ref-10)
10. <http://nvd.nist.gov/> [↑](#footnote-ref-11)
11. <http://www.us-cert.gov/cas/signup.html> [↑](#footnote-ref-12)
12. <http://csrc.nist.gov/publications/PubsSPs.html#800-92> [↑](#footnote-ref-13)
13. Incident handlers should log only the facts regarding the incident, not personal opinions or conclusions. Subjective material should be presented in incident reports, not recorded as evidence. [↑](#footnote-ref-14)
14. If a logbook is used, it is preferable that the logbook is bound and that the incident handlers number the pages, write in ink, and leave the logbook intact (i.e., do not rip out any pages). [↑](#footnote-ref-15)
15. NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response, provides detailed information on establishing a forensic capability. It focuses on forensic techniques for PCs, but much of the material is applicable to other systems. The document can be found at <http://csrc.nist.gov/publications/PubsSPs.html#800-86>. [↑](#footnote-ref-16)
16. Evidence gathering and handling is not typically performed for every incident that occurs—for example, most malware incidents do not merit evidence acquisition. In many organizations, digital forensics is not needed for most incidents. [↑](#footnote-ref-17)
17. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, from the Computer Crime and Intellectual Property Section (CCIPS) of the Department of Justice, provides legal guidance on evidence gathering. The document is available at <http://www.cybercrime.gov/ssmanual/index.html>. [↑](#footnote-ref-18)
18. Metrics such as the number of incidents handled are generally not of value in a comparison of multiple organizations because each organization is likely to have defined key terms differently. For example, most organizations define “incident” in terms of their own policies and practices, and what one organization considers a single incident may be considered multiple incidents by others. More specific metrics, such as the number of port scans, are also of little value in organizational comparisons. For example, it is highly unlikely that different security systems, such as network intrusion detection sensors, would all use the same criteria in labeling activity as a port scan. [↑](#footnote-ref-19)