We the People
insure domestic Tranquility, provide for the common defence
and our Posterity, do ordain and establish this Constitution for
Article I

Federal Continuity Directive

Federal Executive Branch Continuity Program Management Requirements

FEMA Office of National Continuity Programs

August 2024

U.S. DEPARTMENT OF HOMELAND SECURITY
FEMA

This page intentionally left blank

Table of Contents

1. Applicability and Scope

In accordance with Presidential Policy Directive 40 (PPD-40), *National Continuity Policy*, the provisions of this Federal Continuity Directive (FCD) apply to federal executive departments and agencies (D/As) enumerated in 5 United States Code (U.S.C.) § 101, government corporations as defined by 5 U.S.C. § 103(1), independent establishments as defined by 5 U.S.C. § 104(1), the intelligence community as defined by 50 U.S.C. § 3003, and the U.S. Postal Service (USPS). The D/As, boards, bureaus, commissions, corporations, foundations, and independent organizations are hereinafter referred to as "organizations" to better reflect the diverse organizational structures within the Federal Executive Branch.

The FCDs apply to the whole of each Federal Executive Branch organization, in coordination with external essential functions and services partners. Organizations are accountable for their essential functions and the associated development of requirements for their subordinate elements. Given that risk mitigation varies from one function and supporting activity to the next, the implementation of this FCD is coordinated by the respective organization's Continuity Coordinator in support of the organization's Mission Owners and organizational leadership risk management decisions. The organization's leaders, including the Continuity Coordinator and Mission Owners, determine the extent to which the principles outlined in the FCDs apply to components, regional offices, or field offices.

In this FCD, the term "headquarters" (HQ) refers to an organization's central head office of operations for either or both essential functions and command and control. The terms "component" and "subcomponent" refer to all organizational elements, whether at HQ or a regional or field office.

Unless otherwise specified, the annual requirements of this FCD are defined as those scheduled to occur during the federal fiscal year, Oct. 1 through Sept. 30.

1.1. Supersession

This FCD rescinds and supersedes FCD-1, *Federal Executive Branch Continuity Program and Requirements*, January 2017, and *FCD-1 Implementation Scoping Guidance*, January 2018.

2. Handling

2.1. Distribution

This FCD is distributed to the heads of all federal organizations, senior policy officials, emergency operations planners, Continuity Coordinators, Continuity Program Managers, Mission Owners, and other interested parties. It may be released through public, unrestricted channels.

2.2. Operations Security

Operations Security (OPSEC), Information Security (INFOSEC), Cyber Security, and other programs are applied to protect against an evolved threat environment targeting federal and state, local, tribal, and territorial (SLTT) organizations and critical infrastructure continuity plans and programs. They consist of systematic processes that help organizations deny potential adversaries information about their capabilities and intentions by identifying, controlling, and protecting generally unclassified information associated with the planning and execution of sensitive activities. Organizations must implement comprehensive security measures to protect continuity plans, programs, Staff and Organization, Equipment and Systems, Information and Data, and Sites against hostile actions. Such security measures include identifying critical information, conducting risk analyses, and applying appropriate physical, communications, information, and personnel security measures and countermeasures.

Personnel must report threats, events, and/or suspicious activity directed against the organization's operations by following its security reporting protocols. The Department of Homeland Security's (DHS) National Threat Evaluation and Reporting (NTER) Program Office empowers organizations to adapt to new threats.[1]

In accordance with National Security Presidential Memorandum 28 (NSPM-28), *National Operations Security Program*, January 2021, organizations must establish cooperation between the organization's OPSEC program and its continuity of operations elements to ensure effective coordination of the organization's Mission Essential Functions (MEFs) and the agency's critical information.

The *Department of Homeland Security Federal Emergency Management Agency Security Classification Guide 100.3* establishes key requirements for the handling of federal continuity information and is available through organizational HQ Continuity Program Managers.

[1] National Threat Evaluation and Reporting Program Office | Homeland Security (dhs.gov)

2.3. Point of Contact

For assistance with the information contained in this FCD, please contact the FEMA Office of National Continuity Programs (ONCP) at FEMA-NationalContinuity@fema.dhs.gov.

3. Executive Summary

This FCD, *Federal Executive Branch Continuity Program Management Requirements*, provides direction and establishes the minimum requirements for organizations to build and maintain a viable continuity program and increase the resilience of the U.S. Government. Continuity is an inherent part of an organization's day-to-day activities. To better prepare for, respond to, and recover from a disruption, organizations must adhere to the requirements and standards presented in this directive. Leadership, Continuity Coordinators, and Mission Owners must coordinate and apply them to the organization to ensure resilience and the continued performance of essential functions and supporting services under all conditions. All Federal Executive Branch organizations, regardless of their size or location, must have a viable program based on this directive.

The following serve as guiding principles for this FCD to allow organizations to continuously adapt based on their experiences with each new threat and hazard:

- Scalable, flexible, and adaptable continuity programs;
- Leadership engagement and accountability;
- Whole community integration and engagement; and
- Preparedness and essential function resilience alignment.

Continuity programs exist to coordinate and support essential function resilience capability building and evaluation. These activities are accomplished by applying the continuity planning framework, composed of four interconnected planning factors—Staff and Organization, Equipment and Systems, Information and Data, and Sites—across the time-sequenced phases of continuity. By applying these concepts, the Federal Executive Branch can collectively advance the goal of a more resilient nation.

4. Background

This FCD is one of a series of new and revised FCDs that provide direction and guidance for the Federal Executive Branch. It builds on the foundations set forth in *FCD: Continuity Planning Framework for the Federal Executive Branch*, including the continuity planning framework, which is composed of four interconnected planning factors: Staff and Organization, Equipment and Systems, Information and Data, and Sites. Organizations must consider the four factors to assess and address the risks to their essential functions as outlined in *FCD: Federal Executive Branch Essential Functions Risk Identification and Management*.

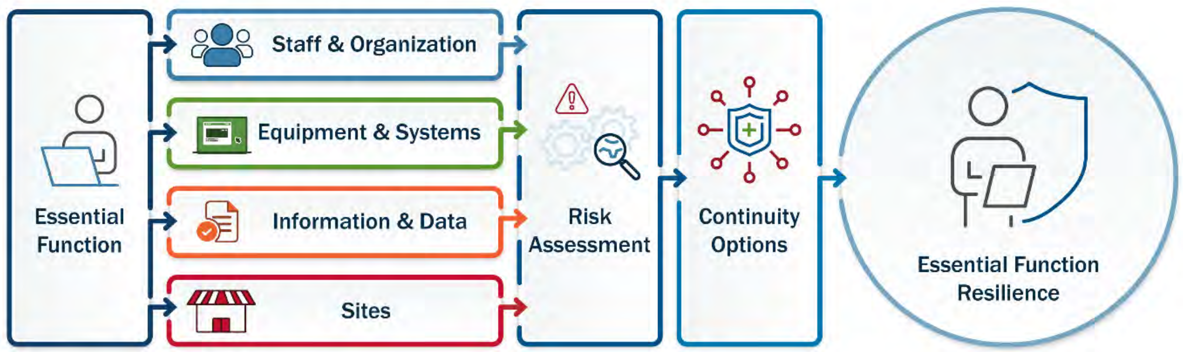


Figure 1: Continuity Planning Framework

4.1. Purpose

This FCD provides direction and guidance for administering an organization-level continuity program within the continuity planning framework. These programs are charged with coordinating and supporting Mission Owners and other leadership to ensure the continued performance of essential functions in accordance with mission requirements. These requirements range from no-downtime to other no-fail functions with a much longer downtime and require robust organizational program management processes to effectively mitigate the risks and ensure U.S. continuity of government (COG).

4.2. Policy

PPD-40, *National Continuity Policy*, outlines the overarching continuity requirements for the Federal Executive Branch and directs the Secretary of Homeland Security, through the FEMA Administrator, to coordinate the implementation, execution, and evaluation of continuity activities among Federal Executive Branch organizations. Specifically, it directs the FEMA Administrator to develop and publish FCDs to establish continuity program and planning requirements. This FCD and others fulfill that requirement.

The goal of **national continuity policy** is the preservation of government structure under the United States Constitution and the continued performance of National Essential Functions (NEFs) under all conditions.

5. Continuity Roles, Coordination, and Collaboration

Leaders provide organization-wide vision and direction and set goals. Continuity Coordinators and Mission Owners are leaders specifically designated to direct and manage the organizational continuity program and essential functions, respectively, and integrate National Continuity, including Federal Mission Resilience, concepts into day-to-day operations. They must coordinate and collaborate with other leaders internal and external to the organization, including management and the federal and contracted staff, to ensure the performance of essential functions.

Leadership Engagement and Accountability: Continuity Program

Leaders are those responsible for the performance of operations, including the delivery of services and/or products. They must integrate essential function resilience concepts into the continuity program and identify the resources, including funding, needed to sustain operations through impact.

5.1. Roles and Requirements

Organizations must appoint a Continuity Coordinator for organizational continuity program coordination and designate Mission Owners for each essential function. The Continuity Coordinator shall designate a Continuity Program Manager to assist them in their duties, particularly those associated with the day-to-day management of the program.

- **Continuity Coordinator:** A senior accountable Federal Executive Branch official, at minimum an Assistant Secretary or equivalent level as defined by 5 U.S.C. § 5315, who ensures continuity capabilities in the organization and provides recommendations for continuity policy. Continuity Coordinators are supported primarily by the Continuity Program Manager and by other planners or coordinators at their subordinate levels throughout the organization. As the organizational official responsible for coordinating with internal leaders and national continuity leadership, the Continuity Coordinator must, among other requirements:

    - Represent the organization on the Continuity Advisory Group (CAG) (see Section 5.2.1);
    - Coordinate across the Federal Executive Branch to understand the interdependencies of the organization’s Primary Mission Essential Functions (PMEFs) and MEFs;
    - Advocate for the continuity program within the organization; and
    - Ensure continuity requirements are integrated into the organization’s strategic planning or budget submission processes.

    The Deputy Secretary (or equivalent) shall meet with their Continuity Coordinator to discuss internal continuity matters and mission resilience at least quarterly, although more frequent engagement is recommended. During these meetings, they should identify, as necessary, risks with the potential to impact enterprise essential function operations and continuity programs, as well as issues affecting the organization and the resources needed to support those functions and programs.

- **Continuity Program Manager**: The individual responsible for managing day-to-day continuity programs and reporting to the Continuity Coordinator on all continuity program activities, such as policy revisions, planning efforts, training and evaluation cycles, and interagency coordination. This individual may also be designated to represent the organization on the CAG and other working groups, or have other duties delegated to them by the Continuity Coordinator as deemed appropriate by the organization's leadership. The Continuity Program Manager supports organizational components to ensure that continuity plans can be executed with little or no notice. This includes coordinating and managing activities that ensure the performance of essential functions and identifying and budgeting resources across the four continuity planning factors.

- **Mission Owner**: An individual accountable for performing an essential function that must be sustained during or quickly resumed following a disruption to normal operations. For the Federal Executive Branch, this is the senior accountable government position with the original or delegated authority to lead the Planning, Programming, Budgeting and Execution (PPBE) (see Section 7.1.1) and associated risk management of a specific essential function. Mission Owners must, among other requirements:

  - Lead the business process analysis (BPA), risk assessment/business impact analysis (BIA), and ongoing risk mitigation efforts for their essential function, as established in *FCD: Federal Executive Branch Essential Functions Risk Identification and Management*;
  - Ensure that continuity requirements are integrated into the strategic planning, operational planning, and budgeting processes for each of their accountable essential functions;
  - Support organization-wide continuity planning and preparedness initiatives; and
  - Identify and communicate to the Continuity Coordinator and/or Continuity Program Manager any needs for technical assistance, organization-level risk mitigation initiatives, or other support.

Continuity Personnel: Roles and Responsibilities

During a disruption to normal operations, organizations mobilize specific, pre-identified personnel. These designated "continuity personnel" consist of the leadership, staff, and functional support elements designated to enable the continued performance of essential functions. They may be organized to perform or support the continued performance of essential functions through distribution, devolution, relocation, or hardening options that can withstand key vulnerability impacts.

See Annex A: Staff and Organization for more information on the roles and responsibilities of continuity personnel.

5.2. Coordination and Collaboration

Organizations must work collaboratively to promote the development, coordination, and integration of continuity plans and programs. These partnerships improve resilience and enhance cooperation through shared experiences and resources across the federal and non-federal landscapes.

5.2.1. FEDERAL EXECUTIVE-LEVEL CONTINUITY AND GOVERNANCE COORDINATION MEETINGS

Federal executive-level continuity coordination meetings are designed to serve as forums for promoting the development, coordination, and integration of continuity planning and programs within the Federal Executive Branch. Continuity Coordinators, Continuity Program Managers, and Mission Owners work collaboratively to plan and coordinate the implementation of national continuity policy within their respective organizations. The National Continuity Coordinator (NCC) is responsible for coordinating, without exercising directive authority, the integration and execution of national continuity policy. The following forums are intended to support the NCC in this capacity:

- **Continuity Advisory Group:** The CAG is an interagency policy coordination group chaired by FEMA ONCP and co-chaired on a rotating basis by a member organization. Through the CAG, FEMA provides a Federal Executive Branch forum that coordinates and addresses all aspects of national continuity policy, planning, operations, training, exercise, and assessment. The FEMA ONCP Associate Administrator is supported by the CAG Steering Committee Chair and the FEMA ONCP CAG Program Management Office, who administer the interagency body and constituent Interagency Continuity Working Groups (ICWGs).

- **Interagency Continuity Working Group:** ICWGs are issue-specific working groups chartered under the CAG governance structure. They are designed to bring together subject-matter experts from across the Federal Executive Branch to review, address, and implement requirements outlined in current or emerging national continuity policies. ICWGs provide a robust and organized means of coordinating the review, revision, and implementation of continuity planning, policy, training, exercise, and assessment activities.

- **Small Agency Council Continuity of Operations Committee:** This is a forum for the review, coordination, and implementation of national continuity policy among Category IV D/As. FEMA ONCP assists the committee in meeting the unique national continuity policy, planning, training, exercise, and assessment challenges of these Category IV organizations, at the request of the committee chair.

5.2.2. FEDERAL AND NON-FEDERAL COORDINATION AND COLLABORATION

Continuity is not strictly a governmental responsibility, nor is it limited to specific disciplines. It must encompass a culture that reaches across the whole community. Governmental leadership at all levels should consider the role of both private-sector and nonprofit organizations as well as individuals.

Whole Community Integration and Engagement

Resilient essential functions require planning and coordination efforts that surpass organizational boundaries, as well as input from all organizations involved in the performance of a function. Organizations must engage and collaborate across the whole community—federal, SLTT, private-sector, and nonprofit entities—to manage risk to essential functions and services.

All advisory committees formed by federal organizations must comply with the Federal Advisory Committee Act, as amended (5 U.S.C. §§ 1001–1014).

Federal Executive Branch organizations should collaborate to further increase their ability to perform essential functions and services. This enables them to share resources without delay, regardless of threats or conditions, and with the understanding that adequate warning of a threat may not be available. The following are examples of collaboration:

- Partnering to align resources more effectively and efficiently across organizational boundaries and mission areas;
- Participating in working groups, information-sharing mechanisms, and training activities, as appropriate;
- Collaborating with other entities to share best practices when developing continuity training and evaluation activities;
- Developing memoranda of agreement/understanding (MOAs/MOUs) and interagency agreements (IAAs) with other organizations to gain or share capabilities and resources;
- Coordinating and collaborating on risks and challenges to identify threats and hazards relevant to the organization’s mission, the location(s) where essential functions are performed, and dependencies;
- Coordinating continuity plans, Occupant Emergency Plans (OEPs), and local/regional evacuation plans;
- Partnering with other organizations on alert and notification networks and credentialing initiatives;
- Collaborating to identify interdependencies and ensure critical infrastructure resilience at all levels; and
- Coordinating security resources and requirements, as appropriate.

Organizations must coordinate and integrate continuity programs across all levels of government, nongovernmental organizations (NGOs), and critical infrastructure sectors to sustain national continuity policy. SLTT governments provide for and serve the public through the assurance and delivery of essential services during catastrophic emergencies. SLTT government resilience creates the foundation for and enhances the effectiveness of federal continuity, which enables the conduct of response and recovery operations.

FEMA integrates continuity and resilience requirements and incentives into FEMA SLTT grant guidance to encourage jurisdictions to develop viable continuity plans. Such plans are needed to ensure the performance of essential functions and sustain the delivery of essential services and core capabilities. Federal organizations, as applicable, will coordinate with SLTT governments, regional entities, and critical infrastructure sectors to promote integration and collaboration.

Sharing and Safeguarding Information in Collaborative Environments

Controlled unclassified information (CUI) is sensitive information that does not meet the criteria for classification but must still be protected. Organizations should consider OPSEC guidance, wherever feasible, to ensure that all materials, resources, and information shared for an authorized lawful government purpose with whole community partners are properly labeled, secured, and maintained.

6. Essential Functions

Each Federal Executive Branch organization must identify its essential functions and analyze the resources and processes needed to perform them. It must also identify the risks to these functions and decide how best to mitigate them.

Essential function resilience is the outcome of effectively managing risks to Staff and Organization, Equipment and Systems, Information and Data, and Sites so vulnerabilities to essential functions have been mitigated and any degradation or delay in the function's performance is within tolerable thresholds.

The collective functions of Federal Executive Branch organizations are called Government Functions. Essential functions are subsets of these Government Functions that are categorized as Mission Essential Functions, Primary Mission Essential Functions, and National Essential Functions.

- **MEFs**: The essential functions directly related to accomplishing the organization's mission as set forth in its statutory or executive charter that are unique to each organization.
- **PMEFs**: The MEFs that must be continuously performed to support or implement the uninterrupted performance of NEFs.
- **NEFs**: Select functions that are necessary to lead and sustain the Nation during a catastrophic emergency and therefore must be supported through continuity of operations, COG, and enduring constitutional government (ECG) capabilities.

The organization's Government Functions that directly accomplish its enduring, organizational-level mission and cannot be deferred, even during a disruption of normal operations, are its MEFs. If a MEF also supports or implements any of the NEFs (detailed below), the organization identifies it as a candidate PMEF for review and coordination by the Interagency Board (IAB).

National-level coordination enables the continuous performance of NEFs. The NEFs are shown in Figure 2.

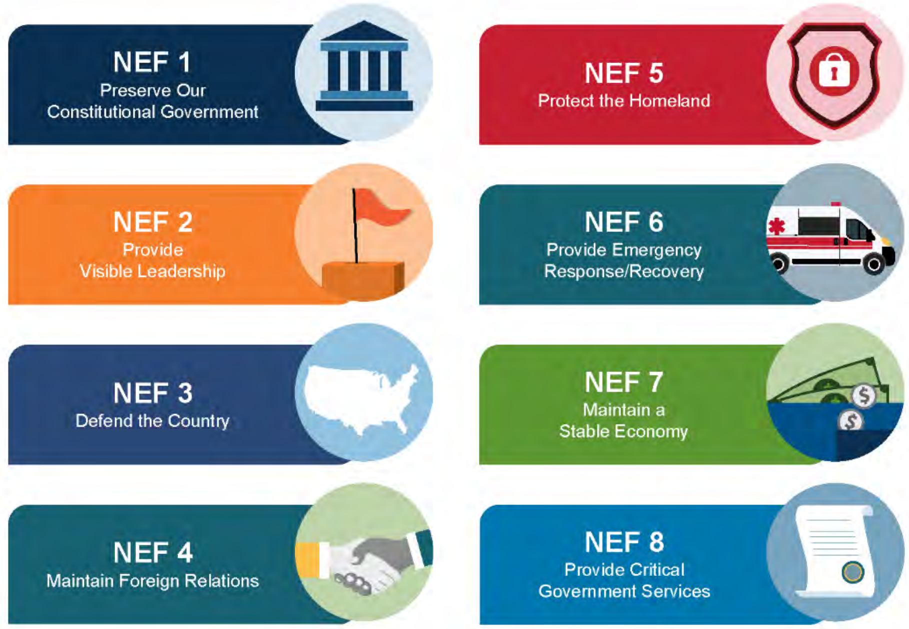

NEF 1
Preserve Our Constitutional Government
NEF 5
Protect the Homeland
NEF 2
Provide Visible Leadership
NEF 6
Provide Emergency Response/Recovery
NEF 3
Defend the Country
NEF 7
Maintain a Stable Economy
NEF 4
Maintain Foreign Relations
NEF 8
Provide Critical Government Services

Figure 2: National Essential Functions

After leadership identifies and validates MEFs, the organization conducts a BPA of the MEFs. A BPA is a systematic method of examining, identifying, and mapping the processes, continuity planning factors (Staff and Organization, Equipment and Systems, Information and Data, and Sites), and other resources (including budget) needed to perform a MEF. The BPA also identifies essential supporting activities (ESAs), which are select mission support activities that enable or facilitate the performance of its essential functions. Organizations may also identify tasks that support the performance of MEFs and ESAs. These tasks may be referred to by unique names specific to the organization.

The organization then conducts a BIA to assess risk to each of its essential functions. The BIA provides a method of identifying threats and hazards that may impact the performance of these functions, along with problem areas such as resource gaps, process weaknesses, consolidated points of failure, and other vulnerabilities.

This analysis enables the organization to identify continuity options (such as distribution, devolution, relocation, and hardening) to close gaps and address vulnerabilities and potential consequences for the performance of its essential functions. It also allows the organization to prioritize investments that improve its own essential function resilience.

Identifying and Managing Risk to Essential Functions

For more information on how to accomplish the requirements in this section, please see *FCD: Federal Executive Branch Essential Functions Risk Identification and Management*.

7. Phases of Continuity

Organizations must create and maintain a viable continuity program with comprehensive continuity plans to responsibly guide the activities that ensure the performance of their essential functions and services. A comprehensive continuity planning process must account for four phases (see Figure 3). These phases help to synchronize the plan in time, space, and purpose. The plan builds continuity processes, outlines goals, and supports the performance of organizational essential functions during a disruption to normal operations.

The four phases of continuity are **Readiness and Preparedness**, **Activation**, **Continuity Operations**, and **Establishing a New Normal**.

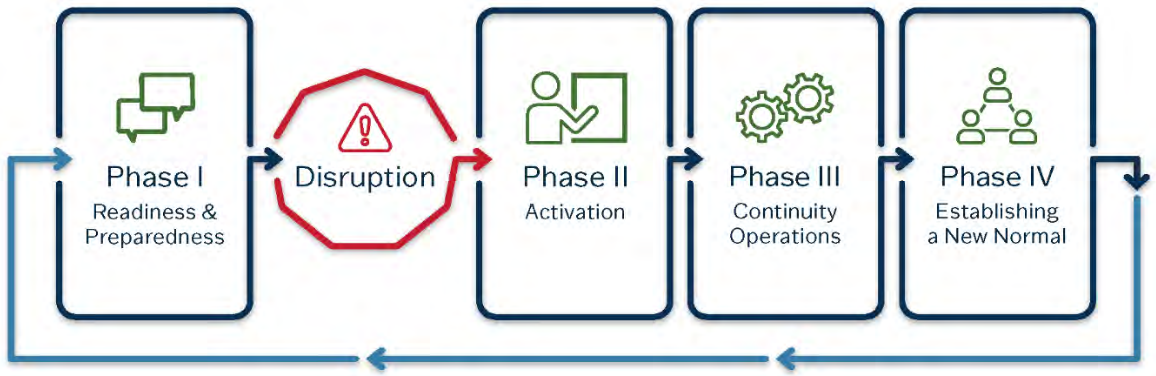


Figure 3: The Four Phases of Continuity

7.1. Phase I: Readiness and Preparedness

Readiness is the condition of being prepared and capable to act or respond as required. Preparedness is the development and sustainment of the capabilities needed to prevent, protect against, mitigate, respond to, and recover from all threats, hazards, and incidents. All levels of leadership are ultimately responsible for ensuring that the organization can perform essential functions before, during, and after a disruption.

The Readiness and Preparedness phase includes the following activities:

- Establishing and maintaining a continuity program;
- Developing, reviewing, and revising plans;
- Identifying essential functions;
- Identifying and managing risks;
- Conducting essential function evaluation activities, including testing and exercising;
- Providing training to all staff and promoting personal preparedness;
- Conducting corrective action planning and execution; and
- Submitting Continuity Status Reports (CSRs).

Preparedness and Essential Function Resilience Alignment

Effective preparedness activities can be achieved through a standardized program management process that prioritizes the investment in essential function resilience.

7.1.1. PROGRAM MANAGEMENT

A standardized continuity program management process provides consistency across organizations' continuity programs to ensure the performance of essential functions during a disruption to normal operations. It guides organizational leadership to allocate sufficient resources to support the program requirements. It must, at minimum, account for the following objectives:

- Identify the processes, resources, and dependencies that support essential functions and activities, and incorporate risk management across the program, including identifying and assessing potential threats and hazards as well as their associated impacts.
- Make informed decisions regarding acceptable levels of risk and identify the required mitigation resources with which to apply appropriate continuity options.
- Seek to improve resilience, including through investments that mitigate acknowledged challenges, and close self-identified gaps.
- Through evaluation, assess and validate continuity policies, plans, procedures, and operational capabilities.
- Train personnel required to support the continued performance of essential functions to ensure they understand how to execute their assigned operational role during continuity plan activation.
- Document the use of plans during tests, exercises, and real-world events by conducting after-action reviews and implementing corrective action efforts that address gaps and shortfalls in plan execution.
- Ensure that continuity options are incorporated as a fundamental part of day-to-day operations so that operational success is achieved and essential functions continue to be performed.

Organizational leadership, including Continuity Coordinators and Mission Owners, must actively work together to create essential function resilience. Organizations should leverage a concept such as, PPBE and resource allocation planning cycles to allocate resources, make decisions, and communicate program priorities. PPBE is an annual process focused on financial and resource management composed of four interconnected phases:

- **Planning:** The process of defining and articulating strategies to inform operational activities and programmatic resource planning as a short- and long-term effort. This phase allows continuity programs to assess changing threat, technology, and economic conditions and to illustrate the short- and long-term budget and strategic planning implications.
- **Programming:** The process of translating organizational priorities and strategic guidance into specific resource allocation decisions over a multi-year period. This phase allows continuity programs to define and analyze investments, construction, human capital, information

technology (IT), and other support and operating expenses with their multi-year resource implications and the evaluation of various trade-offs.

- **Budgeting:** The process of developing a budget—including the formulation, justification, execution, and control of the budget—for submission to organizational leadership and budget approval bodies. The purpose is for organizations to acquire the resource funding needed to ensure the resilience of essential functions.
- **Execution:** The process by which organizations allocate resources, identify costs, and monitor performance to determine the value and impact of essential function performance. Organizations will regularly review and report expenditures to ensure alignment with strategic and leadership priorities.

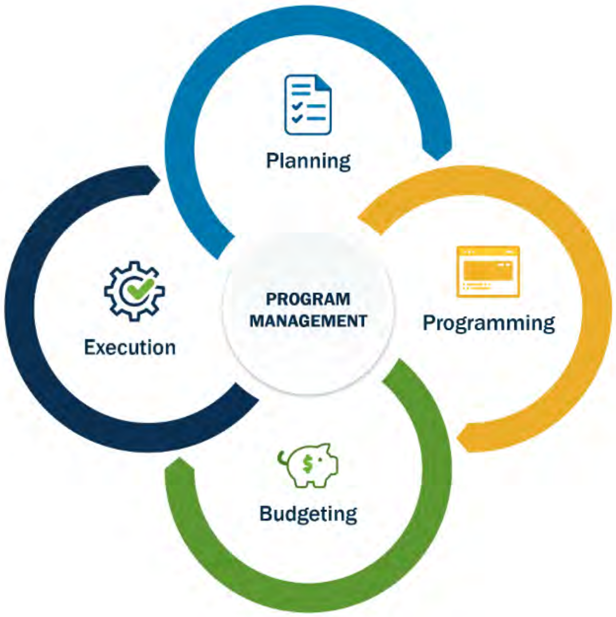


Figure 4: PPBE Cycle

PPBE: Planning

Organizations should develop a Multi-Year Strategic Plan (MYSP) managed by the Continuity Program Manager or designee to provide for the development, maintenance, and annual review of continuity plans, policies, and procedures. It should include the following, at a minimum:

- Multi-year (three to five years) goals, objectives, and leadership guidance for the maintenance and continuous improvement of the program;
- A project plan with associated dates/milestones as well as resource and funding considerations;
- Procedures to regularly monitor and report progress and actions and to determine how accomplishments will be assessed;
- Potential program implementation issues, concerns, and obstacles, as well as a remediation strategy; and

- Planning, training, evaluation, and corrective action, as well as continuous improvement milestones and activities.

A MYSP with short- and long-term goals and objectives serves as a framework for making decisions and provides a basis for planning. By analyzing the information in the strategic plan, leadership, Mission Owners, and continuity planners can make the necessary changes and set the stage for further project planning.

Continuity Program Management Resources

Continuity Program Managers may refer to ONCP's *Guide to Continuity Program Management*,[2] accessible in the FEMA Continuity Resource Toolkit.[3] The guide provides templates and guidance for developing a MYSP, project plans, and a multi-year program evaluation calendar.

PPBE: Programming

Organizations should build on the MYSP to establish program management and execution metrics and monitor the specific tasks that need to be accomplished to ensure the program remains viable and successful. Continuity programs should establish and analyze acquisitions or investments necessary for staff, equipment and systems, information and data, and site construction or maintenance projects. These programs should plan for operating expenses to meet the multi-year goals outlined in their MYSP, within the stated fiscal constraints, and consider various trade-offs.

PPBE: Budgeting

Essential function resilience requires continuity programs to invest in strategies that mitigate challenges, threats, and hazards and aim to close gaps and address vulnerabilities. Organizations must work closely with the Office of Management and Budget (OMB) to identify statutory requirements and administrative priorities when assessing the critical continuity resources needed to perform the organization's essential functions before, during, and after any event that causes a disruption to normal operations.

In the development phase of the executive budget process, OMB issues a budget planning guidance memorandum. This provides executive agencies with detailed instructions and deadlines for submitting their budget requests and supporting materials to OMB. The guidance may also include specific instructions for how agency budget requests may help align with the President's budgetary priorities and achieve other policy goals.

[2] FEMA National Continuity Programs - Guide to Continuity Program Management

[3] Continuity Policy, Doctrine and Guidance | FEMA.gov

Circular No. A–11, *Preparation, Submission, and Execution of the Budget*, which is updated annually, provides agencies with an overview of applicable budgetary laws, policies for the preparation and submission of budgetary estimates, and information on financial management and budget data systems.[4] It also provides agencies with directions for budget execution and guidance regarding agency interaction with Congress and the public.[5] Organizations' HQ must ensure that the continuity program is funded at all levels, including regional and field offices as appropriate, and cover the following, at a minimum:

- Identify the funding requirements to accomplish continuity program goals, objectives, and tasks.
- Identify and account for the funding necessary for sufficient staff across the organization and the assets (e.g., Equipment and Systems, Information and Data, and supplies) necessary to support operations from the organization's alternate site or another directed work location (a location other than the official worksite, such as an employee's residence), maximizing workplace flexibilities until normal operations are resumed.
- Establish procedures for emergency procurement of equipment, supplies, services, and personnel to support continuity operations.
- Integrate continuity requirements into existing and future contracts and MOUs/MOAs, as applicable, to ensure the continued performance of essential functions during a disruption to normal operations for a minimum of 30 days or until normal operations are resumed.

Additional actions to achieve resilience include developing and implementing resilient capabilities critical to the performance of essential functions and services (e.g., communications and information systems, critical infrastructure, supply chains); developing disciplined investment plans to modernize key capabilities through geographic diversity or hardening; and revising policy, plans, legislation, and budgetary priorities to reduce risk to essential functions and services. To explore these actions, organizations should:

- Leverage low-cost, no-cost, or shared resources;
- Explore government-wide funding sources and opportunities, including pilot programs and potential consolidations or partnerships;
- Identify efficient multi-use technology and resources; and
- Directly address essential functions, continuity requirements, and capabilities within enterprise-level strategic plans and performance management efforts.

Organizations' senior leaders must ensure that each part of the organization is involved in the budgeting effort and held accountable to achieve effective continuity. Senior leaders typically have the authority to direct engagement in the program, determine its budget priorities, and hold personnel across the organization accountable. Leaders at the Secretary and Deputy Secretary (or equivalent) levels are required to engage directly in the budgeting process for programs to ensure

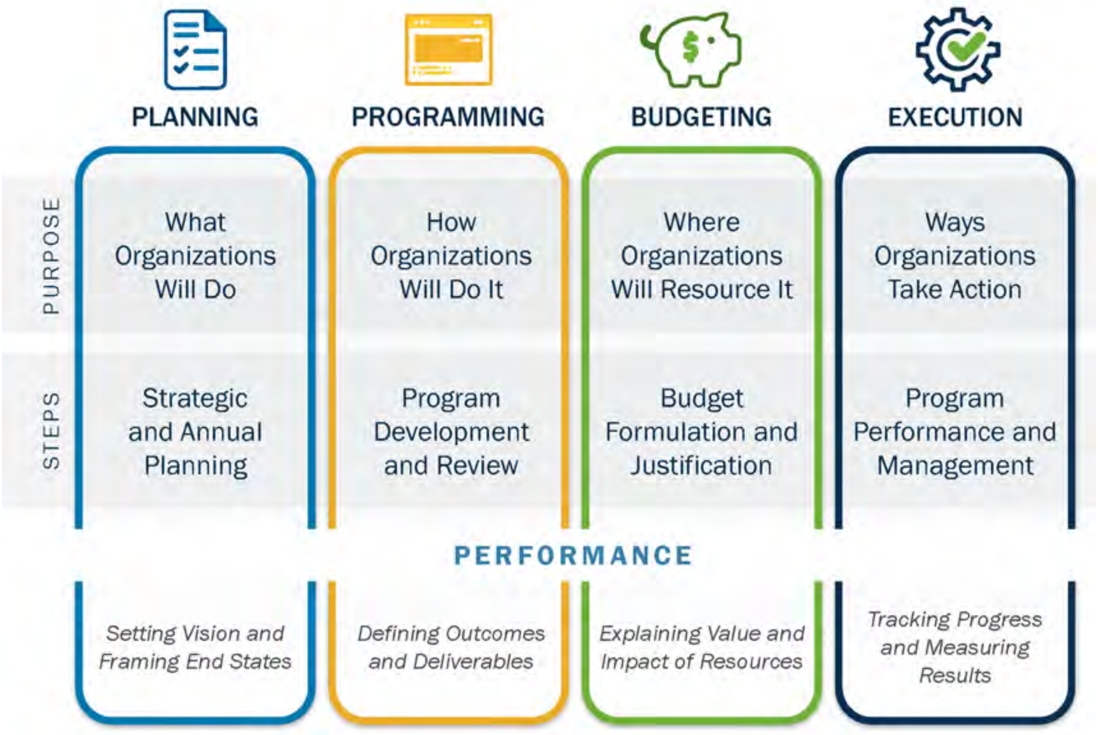
[4] Circular No. A–11.pdf (whitehouse.gov)

[5] The Executive Budget Process: An Overview (congress.gov)

the resilience of essential functions and to make sure that National Continuity, including Federal Mission Resilience, remains at the forefront of all intra- and interagency efforts.

PPBE: Execution

Organizations must use their internal strategic planning and budgeting processes to continuously review the integration of continuity programs into strategic plan objectives, performance metrics, and funding. This evaluation includes examining how well currently available appropriations are being obligated and expended (i.e., measurement of appropriated funds versus the organization's projected costs). However, although that measurement is important, perhaps more important is the comparison between what the organization said it would accomplish with its appropriations and what it accomplished (i.e., outcomes achieved).



	PLANNING	PROGRAMMING	BUDGETING	EXECUTION
PURPOSE	What Organizations Will Do	How Organizations Will Do It	Where Organizations Will Resource It	Ways Organizations Take Action
STEPS	Strategic and Annual Planning	Program Development and Review	Budget Formulation and Justification	Program Performance and Management
PERFORMANCE	*Setting Vision and Framing End States*	*Defining Outcomes and Deliverables*	*Explaining Value and Impact of Resources*	*Tracking Progress and Measuring Results*

Figure 5: Overview of PPBE Activities

Leadership Engagement and Accountability: PPBE

Program management and PPBE are ultimately the responsibility of leadership. Leaders must ensure that the organization can perform essential functions before, during, and after all-hazards emergencies.

To the extent that the performance goals of an existing program are not being met, the execution review may lead to recommendations to adjust resources and/or restructure programs to achieve the desired performance goals.[6]

Essential function resilience can be achieved only through improving capabilities, reinforcing skill sets, and closing identified gaps. The organization's leadership must champion a program with a continuous improvement process that includes:

- Conducting and documenting comprehensive evaluations of relevant programs/subprograms; and
- Reviewing planned activities for the current fiscal year and providing recommendations for resource allocation for the upcoming fiscal year.

Scalable, Flexible, and Adaptable Continuity Programs

Organizations are required to establish continuity programs that promote multiple options for the seamless continued performance of essential functions as the situation, mission, and functions require. This can include:

- Proactively distributing operations (e.g., staff or sites) and reducing single points of failure across dispersed geographic areas as a full-time posture;
- Establishing procedures for relocating continuity personnel to alternate sites;
- Identifying measurable, data-driven, flexible risk mitigation approaches that address threats and hazards through an informed decision-making process; and
- Sharing resources (e.g., a facility that provides classified communications capabilities) via MOAs/MOUs, standing visit access requests, reciprocity, and IAAs, wherever possible.

The employment of scalable, flexible, and adaptable programs, such as distributing operations to the greatest extent possible, reduces overall risk and the likelihood of impacts to essential functions while acknowledging that not every operation can be distributed and residual risk may be transferred to other areas.

7.1.2. CONTINUITY PLANNING

Federal Executive Branch organizations must develop continuity plans, including plans for devolution and reconstitution, with appropriate delegations of authority for leadership and staff to increase survivability and maintain the performance of essential functions. These plans allow organizations to engage the whole community in considering the life cycle of a potential emergency, determining the

[6] Performance Framework | Performance.gov

required capabilities to maintain essential functions, and establishing a framework for roles and responsibilities. Accordingly, essential functions form the foundation of the organization's plan.

Continuity plans require a process for ensuring the performance of essential functions using geographically dispersed resources and assets. Plans must include:

- Activities required within the four phases of continuity—Readiness and Preparedness, Activation, Continuity Operations, and Establishing a New Normal.
- A process for attaining and reporting the organization's operational capability, reflecting the status of HQ and other facilities, such as regional or field offices, where PMEFs and MEFs are performed.
- A process for determining the organization's operational status and continuity decision-making protocols. Organizations must establish internal procedures for executing changes to directed Readiness Levels, as appropriate.
- Triggers for activation and a decision matrix for activation with warning and without warning during duty and non-duty hours.
- A process or methodology to ensure operations can be sustained for a minimum of 30 days following a disruption to normal operations or until normal operations are resumed. This includes planning for the challenges posed by disruptions to normal operations that extend past 30 days.
- Detailed processes and procedures for the use of continuity options following a disruption to normal operations, including:

    - Activating alternate sites;
    - Activating personnel designated to relocate;
    - Transitioning responsibilities to the personnel designated to accept the organization's devolution; and
    - Using other methods (e.g., initiating emergency telework, rebalancing work across distributed operations sites, or any mix of both devolution and relocation) to support the performance of individual essential functions.

- A summary of the organization's essential functions.
- Documentation of continuity capabilities and operations, including emergency budgeting and acquisition, orders of succession, delegations of authority, organization-level continuity options (including the use of primary, distributed, alternate, and devolution sites), communications, essential records, personnel, and program roles and responsibilities.

The organization's plan must be approved and signed by the Organization Head or deputy. The plan must be reviewed annually and updated as required. The organization must record the date of the review and, at minimum, the name, position title, and contact information of the senior-most person and an alternate who conducted the review.

Steady-State Readiness Reporting

Federal Executive Branch organizations are required to report their continuity readiness each month "in accordance with the nature and characteristics of [their] national security roles and responsibilities"[7] and during disruptions to normal operating conditions, as directed by their respective Continuity Program Managers or as instructed by FEMA ONCP guidance. The continuity readiness reporting process ensures a routine and ongoing understanding and assessment of organizations' readiness to perform their essential functions. It also provides Federal Executive Branch leadership and policymakers with relevant, timely, and actionable continuity planning and readiness information and assessments to directly support executive decision-making during a steady state, national-level exercises, and real-world events.

So that FEMA can establish and develop accurate and timely reporting on the status of the Federal Executive Branch continuity readiness, FEMA ONCP has developed a reporting process that requires all Category I, II, III, and IV D/As to submit Quick Look (QL) reports and CSRs:

- Monthly;
- For exercises that include reporting activities or the occurrence of real-world events;
- Upon a directed change in the Readiness Level; and
- During incidents that might trigger partial or full activation of the organization's continuity plans and related continuity options.

Continuity readiness reporting is the collection and management of routine exercise-based or event-specific information and data via the submission of CSRs, Emergency Notification System (ENS) qualification reports, and Federal Continuity Assessment Tools (FCATs). These reports enable ONCP to implement national continuity policy reporting requirements and identify trends in Federal Executive Branch organization readiness to sustain essential functions under all conditions.

Continuity Status Reports

CSRs track federal continuity readiness status and select capabilities under all conditions, specifically focusing on the following requirements:

- Capacity to perform PMEFs and MEFs;
- Status of continuity information and communication capabilities;
- Status of leadership;
- Status of primary and alternate sites (including telework/remote work sites, devolution sites, and co-location facilities);
- Status of the organization's ability to achieve a directed Readiness Level change, as needed; and
- Reports by organizations regarding any issues, concerns, gaps, challenges, vulnerabilities, changes in planning requirements, or identified mitigation measures.

[7] Presidential Policy Directive 40 (PPD-40), *National Continuity Policy*, Section 14, Part (f), July 15, 2016.

To ensure accurate and timely status report submissions and subsequent executive summary reporting, FEMA ONCP uses five types of CSRs:

- **QL:** A report designed to acknowledge receipt of a directed change in Readiness Level or to quickly inform FEMA ONCP of a disruption to normal operations that could impact the organization's essential functions.
- **Readiness Level Change:** A report designed to confirm that the organization has achieved the directed Readiness Level.
- **Continuity Plan Activation:** A report to inform FEMA ONCP of a full or partial activation of the organization's plan.
- **Monthly Continuity Status:** A monthly, steady-state report to FEMA ONCP in accordance with routine reporting requirements.
- **Return to Normal Operations:** A report to inform FEMA ONCP that the organization's continuity plan is no longer fully or partially activated.

Emergency Notification System Qualification Reports

FEMA uses the ENS to send notifications to select individuals and groups identified by each Federal Executive Branch organization. Many of these messages are critical, but some may be sent for testing notification purposes. All messages are sent to personnel via documented communication devices in a notification cascade that includes emails, phone calls, and text messages. Notified personnel are required to respond via one of these means. Qualification reports provide FEMA ONCP with data on the ability of identified Federal Executive Branch personnel and organizations to receive and respond to critical notifications in a prescribed timeframe. These reports inform an aspect of continuity communications capabilities and readiness.

Federal Continuity Assessment Tool

Federal Executive Branch organizations use the FCAT to assess the effectiveness of continuity plans and programs and the organization's ability to perform the essential functions and services outlined in this FCD. FCAT data is submitted quarterly to FEMA ONCP and can be used to identify emerging trends in individual organizations. The FCAT also assists ONCP with identifying Federal Executive Branch continuity community strengths, areas for improvement, and best practices.

FEMA Federal Continuity Assistance Contact Information

For questions regarding the requirements, guidance, or processes for continuity readiness reporting (including CSRs, ENS messages, and FCATs), please contact FEMA ONCP at FEMA-NationalContinuity@fema.dhs.gov.

7.1.3. CONTINUITY TRAINING

Training provides organizational staff with the knowledge, skills, and abilities needed to accomplish the tasks required to perform essential functions. The organization must incorporate continuity requirements into its organization-wide training program. It should make training decisions based on priorities derived from leadership, Mission Owners, and the results of previous evaluation activities.

Federal Executive Branch organizations must plan and conduct training to enhance readiness and ensure understanding of the plans, processes, and procedures regarding the Staff and Organization, Equipment and Systems, Information and Data, and Sites needed for the performance of essential functions.

> Training familiarizes personnel with their roles and responsibilities to support the performance of the organization’s continuity operations. It results in an increased understanding of the organization’s program, processes, and procedures.

The organization’s continuity training must include and document the following:

- Annual continuity awareness briefings for the entire workforce, including new personnel as they onboard. Organizations may consider delivering continuity awareness material in the following ways:
  - Training modules on the organization’s learning management system; and
  - Briefings provided to and reviewed by new hires.
- Annual training on roles and responsibilities for all continuity personnel who are assigned to activate, support, and/or sustain essential function operations, including ESAs. Training must include:
  - Individual-level training on their position-specific responsibilities and tasks and the use of continuity capabilities such as contingency communications equipment, alternate sites, and access to backup records;
  - Organizational continuity plans that involve using or relocating to alternate sites or other work arrangements, such as telework;
  - Reconstitution plans and procedures to resume normal operations at a primary operating facility, a temporary location, or a replacement primary operating facility;
  - Communications and IT system planning necessary to support or sustain continuity operations; and
  - Procedures to identify, protect, and make available the electronic and hard copy essential records, documents, references, and records; information systems; and data management software and equipment (including classified and other sensitive data) needed to support or sustain continuity operations.

- Annual training for the organization's leadership on relevant threats and hazards, essential functions, succession, continuity communications, and deployment requirements.
- Annual training for all organizational and subcomponent personnel designated within the organization's orders of succession or other key positions who assume the authority and responsibility of the organization's leadership if that leadership is incapacitated or becomes otherwise unavailable during a continuity activation.
- Annual training for those officials listed in the delegations of authority on all pre-delegated authorities, including limitations, conditions, and restrictions that have been delegated.

Continuity Training Management

Initial and recurring training informs and familiarizes leaders and staff with continuity plans and procedures. The Continuity Program Manager must:

- Review training completion metrics and learner feedback to evaluate if training improvements are needed.
- Assess the effectiveness of training through evaluation of exercises and real-world event reporting to determine if learning outcomes have been achieved or if more training is necessary.
- Document all training events, including the date of the event, participants, and outcomes. During biennial (every two years) organizational assessments, documentation must be made available to FEMA evaluators.
- Incorporate threats, hazards, and vulnerabilities identified through organizational risk assessments into continuity training.
- Conduct and document a debriefing or hot wash after training events. This may take the form of a survey to allow participants the opportunity to identify strengths and weaknesses in materials and to recommend revisions to the organization's training and continuity plans.

Continuity Training Resources

FEMA has developed the National Continuity Training Program, which provides continuity training resources as well as a library of references, program tools, and document templates.[8]

7.1.4. CONTINUITY EVALUATION

An evaluation program enables organizations to prepare and validate continuity plans and programs and to verify the effectiveness of their risk mitigation efforts by measuring their ability to perform essential functions during a disruption to normal operating conditions.

[8] National Continuity Training Program | FEMA.gov

Federal Executive Branch organizations must plan and conduct routine internal tests and exercises and participate in exercise and evaluation activities. This enables them to monitor continuity capabilities and ensure the adequacy and viability of continuity plans, as well as the Staff and Organization, Equipment and Systems, Information and Data, and Sites needed for the performance of essential functions.

Exercising

Exercises enable the organization to operationally validate the effectiveness of essential function risk mitigation capabilities. They can be used for testing and validating policies, plans, procedures, training, equipment, and IAAs; clarifying and training personnel in roles and responsibilities; improving interagency coordination and communications; improving individual performance; identifying gaps in resources; and identifying opportunities for improvement.

The organization's continuity program must meet the following exercise requirements and document them:

- Annually, all personnel assigned to perform or support a PMEF must validate that all required capabilities are accessible and operational. They do this from an alternate site, devolution site, and/or other location to which they are assigned in continuity plans and procedures.
- Annually (for each PMEF) or biennially (for each MEF), the organization must conduct an exercise to validate its ability to sustain performance of the essential function using one or more continuity options established in its plan(s). As part of these exercises, the organization must:

    - Confirm that the personnel designated to perform or support the essential function have the necessary authorities, training, and other resources required to perform their duties under the organization's continuity plans and procedures.
    - Test and validate the equipment and systems required to perform the function, including intra- and interagency communications capabilities.
    - Verify that the relevant Site and Data and Information resources required to perform and support the essential function are sufficient and accessible.
    - Document exercise findings in an After-Action Report (AAR). The AAR must be validated by the Continuity Coordinator and the Mission Owner(s) of each essential function addressed in the exercise, and the AAR must be made available to FEMA ONCP.

- Annually, each organization must conduct an exercise to validate its ability to sustain command and control of the organization using one or more continuity options established in its plan(s).
- The organization's exercise requirements may be combined with and/or accomplished in conjunction with a FEMA National Continuity Exercise. When participating in a FEMA National Continuity Exercise, organizations must (consistent with the exercise plan):

    - Provide evaluators, data collectors, facilitators, controllers, and other required exercise personnel, as requested;

  - Develop scenario content and injects that enable participants to perform essential functions; and
  - Evaluate the exercise (consistent with the exercise's evaluation plan) and submit findings for inclusion in the overall Eagle Horizon AAR/Improvement Plan (IP).

- Organizations must document all conducted continuity exercise events, including the date and outcomes of the event. During biennial organizational assessments, documentation—including exercise plans, AARs, and corrective action plans—must be made available to FEMA evaluators.

Homeland Security Exercise and Evaluation Program

The Homeland Security Exercise and Evaluation Program (HSEEP) provides a set of guiding principles for exercise and evaluation programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning.[9]

Testing

Tests demonstrate the correct operation of all equipment, procedures, processes, and systems that support the organization's ability to perform essential functions. They ensure that resources and procedures are kept in a constant state of readiness. Testing the organization's policies, plans, and procedures cultivates better organizational knowledge, identifies gaps in coverage, and validates existing plans and programs.

Tests use quantifiable metrics or expected outcomes to validate the operability of critical equipment and systems identified via the organization's BPAs. They can take several forms, including the following:

- **Equipment/component testing:** This tests individual hardware or software components, or groups of related components. A component test might also test processes and procedures that relate to the use of the equipment or component. Organizations should test hardware or software components at the conclusion of their development (but that is not within the scope of this document). Component testing in this document concerns individual components already operational that are critical to the effective operation of the organization and should be regularly tested.

[9] Homeland Security Exercise and Evaluation Program | FEMA.gov

- **System testing:** This tests complete systems to evaluate each system's compliance with specified requirements. A system test should also include an examination of any processes or procedures related to the system being tested.

- **Comprehensive testing:** This tests all equipment and systems that support the organization's essential functions. These tests generally involve multiple components and systems and may become quite extensive in their scope. An example of a comprehensive test is one that confirms that IT operations can be restored at a backup site in the event of an extended power failure at the primary site.

Tests must be conducted in a manner that resembles the everyday work environment in which the system or component is found. If feasible, an actual test of the components or systems used to conduct normal operations for the organization should be used.

The organization's testing program must include and document the following:

- Participation in interagency communications testing activities as established in Office of Science and Technology Policy (OSTP)/OMB Directive D-16-1, *Minimum Requirements for Federal Executive Branch Continuity Communications Capabilities*;
- Alert and notification testing:
  - Monthly testing of alert rosters as well as key partner, stakeholder, and essential function critical point of contact call-down lists; and
  - Quarterly testing of alert and notification procedures for continuity personnel.
- Testing for information systems and essential records:
  - Annual testing of recovery strategies (i.e., disaster recovery plans and/or IT contingency plans) for essential records (both classified and unclassified), critical information systems (both classified and unclassified), services, and data; and
  - Annual testing of information systems (both classified and unclassified) and access to essential records at alternate sites.
- Quarterly testing of the internal and external interoperability and viability of primary and contingency communications and IT systems;
- Annual testing of primary and backup infrastructure systems and services, such as power, water, and fuel, at alternate sites; and
- Annual testing of telework capabilities as outlined in the organization's plan in support of the performance of essential functions and supporting activities, including the IT infrastructure required to support telework during a continuity activation.

Continuity Evaluation Management

Evaluation is the link between establishing or maintaining continuity capabilities and the resilience of essential functions. Effective evaluation involves planning for and collecting data during training, testing, exercising, and actual disruptions, then analyzing the data and reporting outcomes.

Organizations must incorporate the following requirements into organization-wide continuity evaluation management:

- Document all evaluation events, including the date of the event, participants, and outcomes.
- Utilize an all-hazards approach to affirm the viability of essential functions using the threats, hazards, and vulnerabilities identified through organizational risk assessments.
- Maintain a continuous improvement program (CIP) that tracks the implementation of corrective actions identified in post-exercise improvement plans and issues, reporting at least annually to the Continuity Coordinator, Mission Owners, and enterprise risk management stakeholders to inform ongoing organization- and MEF-level risk assessment efforts.
- Provide FEMA ONCP with FCAT results (quarterly).
- Provide documentation of required items and actions to FEMA evaluators, as requested, during biennial organizational assessments.

Improvement Planning

Improvement planning is a process by which the areas for improvement from the evaluation are turned into measurable corrective actions that strengthen capabilities. The following activities can help shape the organization's preparedness priorities and support continuous improvement:

- Conduct and document a comprehensive debriefing or hot wash after each exercise, which allows participants to identify systemic weaknesses in plans and procedures and to recommend revisions to the organization's continuity plans.
- Develop and execute a CIP to document and track actions that improve the organization's ability to perform essential functions and services.
- Take corrective action in a timely manner and continue to progress on longer-term findings before the organization's next annual continuity exercise.

7.1.5. FEMA NATIONAL CONTINUITY EVALUATION PROGRAM

The National Continuity Evaluation Program (NCEP) reports on the state of U.S. continuity based on the collection and analysis of the information reported through the efforts above. FEMA ONCP, in coordination with partners and stakeholders, evaluates current continuity capabilities and establishes development and sustainment priorities for the whole of government and the private sector in order to strengthen the Nation's ability to perform NEFs under all conditions.

- **Goal:** Strengthen the resilience of NEFs through substantive analytical services enabling evidence-informed actions.

- **Scope:** The NCEP evaluates continuity on a national level. While it draws from data sources based on individual organizations, sectors, and jurisdictions, the outputs are national in focus and designed to inform resilience efforts at all levels of government.

Table 1: National Continuity Evaluation Program

Data Collection Sources	Partners and Stakeholders	Areas of Analysis	National Resilience Priorities
▪ Continuity and risk assessments ▪ AARs of simulated and real-world events ▪ Outputs from studies and pilots ▪ Intelligence and threat information	Sharing data and information; identifying and maintaining lanes of responsibility with: ▪ Organizations as identified in Section 1: Applicability and Scope ▪ FEMA National Preparedness Assessment Division and National Exercise Division ▪ FEMA Regions ▪ Cybersecurity and Infrastructure Security Agency (CISA) and critical infrastructure sectors ▪ Emergency Management Accreditation Program ▪ Whole of government stakeholders ▪ Whole community stakeholders	▪ Identification of continuity strengths and challenges ▪ Capability gaps ▪ Risks to the performance of essential functions	Establishing national resilience priorities: ▪ Federal ▪ State ▪ Territorial ▪ Tribal ▪ Local ▪ Private-sector critical infrastructure owners and operators

7.2. Phase II: Activation

This phase includes assessing potential or actual event impacts, activating plans and procedures for continuing the performance of essential functions, and activating personnel, essential records and databases, equipment, and support involved with these functions. Activating and implementing a continuity plan and its associated procedures through the use of one or a combination of continuity options, including distribution, devolution, relocation, or hardening, is dependent on the incident and its effect on normal operations.

Active and passive triggers assist Organization Heads and continuity personnel in recognizing when plan activation is required and enable a smoother transition to continuity operations.

Active triggers initiate actions because of a deliberate decision by the White House or organizational leadership.

Passive triggers are used when leadership is not available to initiate activation and the required actions are taken in accordance with predetermined criteria being met.

Organizations may activate their devolution plan and use devolution as a short-term option while continuity personnel designated to relocate transition to their alternate site(s).

Examples of scenarios that may require activation of continuity plans and procedures may include, but are not limited to, the occurrence or anticipated occurrence of the following:

- Readiness Level change;
- Nation-state threat or action;
- Cyber incident threat or occurrence;
- National Terrorism Advisory System (NTAS) alert or other credible threat reported by law enforcement;[10]
- Severe weather or other natural phenomena;
- Power or IT outage;
- Building or surrounding area access issues; and
- Staff unavailability.

The activation phase must include, but is not limited to, the following activities:

- Reviewing, assessing, and deciding to activate continuity and/or devolution plans;
- Alerting and notifying personnel, including continuity personnel, mutual aid partners, staff at alternate or distributed sites, staff at subordinate and HQ organizations, all other employees, and stakeholders;

[10] National Terrorism Advisory System | Homeland Security (dhs.gov)

- Opening sites;
- Energizing systems;
- Relocating, if necessary, to alternate sites;
- Devolving, if necessary, to devolution sites;
- Activating remote work/telework procedures;
- Accounting for continuity personnel and other staff;
- Receiving personnel;
- Identifying available organizational leadership;
- Establishing communications; and
- Reporting continuity status changes.

7.3. Phase III: Continuity Operations

This phase includes continuity operations and devolution activities to continue performing essential functions.

7.3.1. CONTINUITY OPERATIONS

This is the phase in which organizations implement and execute the continuity options identified in the continuity plan to ensure the continued performance of essential functions. The operations phase must include, but is not limited to, the following:

- Performing essential functions;
- Continuing to account for personnel, including locating and identifying leadership;
- Establishing communications with interdependent organizations and other internal and external stakeholders, including the media and the public;
- Providing guidance to personnel;
- Coordinating the emergency procurement of equipment, supplies, services, and personnel to support continuity operations;
- Performing and capturing information from regular hot washes or other continuous improvement activities;
- Preparing for the reconstitution of the primary site and establishing a new normal; and
- Reporting continuity status changes, as necessary.

7.3.2. DEVOLUTION

Devolution is the transfer of statutory authority and responsibility from an organization's primary operating staff to other staff to maintain organizational command and control and/or perform essential functions when necessary. It requires the use of scalable, flexible, and adaptable operations techniques and the rapid transfer of authority and responsibility to geographic areas far enough from the primary or alternate site to reduce the likelihood of impacts to essential function performance. Organizations may partially rather than fully devolve by transferring responsibilities for only select essential functions. They may also consider devolving to multiple sites or to distributed personnel by transferring authority and responsibility for specific essential functions to various sites.

Devolution is not a phase of continuity but rather a continuity option to employ in tandem with the relocation of operations or when the relocation of operations is not practical. This option can reduce the likelihood of further impacts to essential functions.

When building a devolution option and organizing personnel responsible for carrying out devolution, organizations must ensure they have a holistic understanding of Staff and Organization, Equipment and Systems, Information and Data, and Sites. Continuity personnel assigned responsibilities in accepting devolution are referred to as the Devolution Emergency Response Group (DERG). These personnel ensure that resources are pre-positioned or available within the accepted timeframe to ensure the performance of essential functions.

For essential functions that must be performed continuously, **devolution** allows for the immediate transfer of authorities and responsibilities with the potential for near-zero downtime, as it does not rely on the relocation of personnel and resources.

Requirements and Criteria for Devolution

Where the devolution option is employed as a risk mitigation measure, the organization must plan for devolution and prepare the DERG to continue performing essential functions and services by providing training and conducting evaluations. Organizations should also consider the development of support documentation such as job aids, standard operating procedures, desk guides, and handbooks. In addition to the requirements listed earlier (see Section 7.1.2), organizations must:

- Develop a plan for a devolution option that details the transfer of statutory authority and responsibility to other staff and/or sites to maintain command and control and/or the continued performance of essential functions when the primary operating staff and/or facilities are not available.
    - Identify both active and passive triggers that initiate the activation and implementation of the devolution plan.
    - Specify how and when direction and control of organizational operations will transfer to and from the devolution site.
    - Determine the necessary resources to facilitate an immediate and seamless transfer of functions to the devolution site.
    - List the necessary resources, such as equipment and materials, to facilitate the performance of essential functions at the devolution site.
    - Understand and apply the continuity planning framework factors—Staff and Organization, Equipment and Systems, Information and Data, and Sites—to ensure the performance of essential functions.
    - List the mandatory reporting requirements detailed earlier (see Section 7.1.2) (e.g., CSRs).
    - Outline procedures for the transition of responsibilities to personnel at the primary operating facilities upon termination of devolution.

- Maintain a roster of trained personnel capable of performing devolution operations (DERG members). The roster should include not only primary personnel but also enough alternates or backup personnel. Rosters must be updated periodically and include, at a minimum, names, offices, email addresses, and government-issued cell phone numbers.
- Provide annual training on the roles and responsibilities for personnel, including host or contractor personnel, who are assigned to activate, support, and sustain devolution operations. Training must include the following:

    - Organizational devolution plan processes and procedures;
    - Communications and IT systems that will be used during devolution operations;
    - Identification, protection, and availability of electronic and hard copy documents, references, records, information systems, and data management software and equipment (including classified and other sensitive data) needed to support devolved essential functions during devolution operations; and
    - A process for how the organization identifies and performs its essential functions during an increased threat situation or after a disruption to normal operations activates the devolution plan.

- Ensure that DERG personnel, from their designated devolution site, annually test that the required capabilities are operational.

    - Familiarize DERG members with devolution plan processes and procedures.
    - Demonstrate familiarity with reconstitution plans and procedures for the original primary operating facility and the replacement primary operating facility.

7.4. Phase IV: Establishing a New Normal

In this phase, organizations transition from the continuity facility to either the normal primary facility, another temporary facility, or a new permanent facility. This can occur through distribution, devolution, or relocation. Organizations then focus on confirming the success of the organization's reconstitution operations and establishing a new normal. Establishing a new normal includes, but is not limited to, the following:

- Establishing that the organization can perform all essential functions and operations at the new or restored facility;
- Returning activated continuity personnel to their normal duty assignments;
- Phasing down continuity facility operations and supervising the return of operations, personnel, records, and equipment to the primary or other operating facility using a priority-based approach;
- Conducting a hot wash and/or after-action conference to gather areas for improvement, strengths, and lessons learned from the organization's response to the disruption;
- Preparing an AAR and incorporating approved recommendations into a CIP; and
- Revising and updating plans, procedures, and checklists, as appropriate.

Table 2: Phases of Continuity

Phase I: **Readiness and Preparedness**	**Phase II:** **Activation**	**Phase III:** **Continuity Operations**	**Phase IV:** **Establishing a New Normal**
▪ Developing, reviewing, and revising plans ▪ Coordinating and sharing information internally and externally ▪ Identifying and managing risks ▪ Evaluating activities and incorporating corrective actions ▪ Ensuring personnel preparedness, including providing guidance to all staff ▪ Submitting QL reports/CSRs	▪ Assessing potential or realized event incident impacts ▪ Implementing continuity plans ▪ Mobilizing personnel ▪ Sending notifications and internal and external messages ▪ Submitting CSRs	▪ Accounting for personnel ▪ Continuing the performance of essential functions ▪ Coordinating and collaborating ▪ Ensuring executive decision support ▪ Submitting CSRs	▪ Establishing that the organization can perform all essential functions and operations at the new or restored site ▪ Phasing down alternate or devolution site operations and supervising the return of operations, personnel, records, and equipment to the primary or other operating site using a priority-based approach ▪ Instructing all personnel on new normal operations ▪ Submitting CSRs

8. Reconstitution

During reconstitution, organizational leadership communicates instructions to all staff and supervises the orderly resumption of operations at the primary site, a temporary site, or a new permanent site. Reconstitution activities, established during the Readiness and Preparedness phase prior to disruption, enable the organization to expedite the return to full and normal operations. Reconstitution activities include, but are not limited to, the following:

- Programming, planning, and budgeting for an effective reconstitution program;
- Developing and maintaining a reconstitution plan or annex;
- Coordinating with partners and service providers to identify external sources of required expertise, such as structural engineers or similar experts, to conduct building safety evaluations and/or damage assessments.
- Assessing the status of the affected site(s), including the facility or facilities;
- Determining how much time is needed to repair the affected site or facility and/or acquire a new site or facility;
- Supervising site or facility repairs;
- Replacing or replenishing products used or depleted during the disruption;
- Notifying decision-makers of the status of repairs, including estimates of when the repairs will be completed;
- Assessing the status of personnel;
- Hiring and training replacement personnel;
- Assessing the status of records;
- Repairing and replacing damaged records; and
- Implementing a priority-based, phased approach to reconstitution.

8.1. Reconstitution Phases

The organization resumes operations by establishing a new normal after a disruption. Although separate from the phases of continuity, reconstitution occurs in parallel with them and is critical to the success of the continuity of operations efforts. There are four phases of reconstitution:

1. **Pre-Event Preparedness:** The preparation and mitigation actions taken prior to a disruptive event, such as developing plans, procedures, checklists, and agreements, as well as appointing a Reconstitution Manager and personnel to serve on reconstitution teams.

2. **Event Planning:** The actions taken immediately following a disruptive event to assess damage, determine applicable reconstitution planning levels, and tailor plans to the situation through the creation of courses of action (COAs) for leadership approval.

3. **Implementation of Reconstitution Operations:** Coordination with partners and service providers and the execution of the organization's approved reconstitution COAs.

4. **End of Reconstitution:** The actions taken upon return to the facility or establishment of a new normal. Hot washes are conducted and documented. AARs are developed, through which plans, procedures, checklists, and agreements are adjusted as needed.

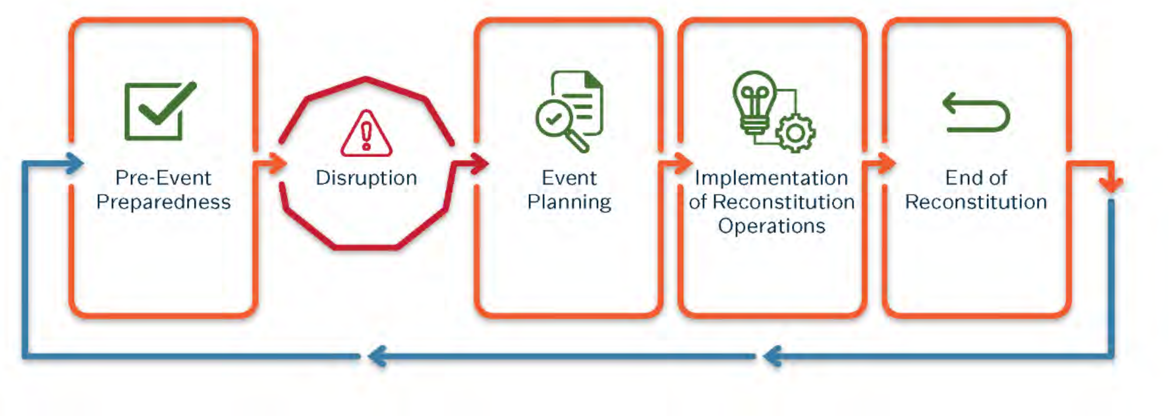


Figure 6: Phases of Reconstitution

8.2. Reconstitution Roles

The *Executive Branch Reconstitution Concept of Operations* outlines the approach to reconstituting the Federal Executive Branch and establishing a new normal following a disruption to normal operations. It defines the roles and responsibilities of organizations, including the key assistance roles played by FEMA, the General Services Administration (GSA), the Office of Personnel Management (OPM), and the National Archives and Records Administration (NARA).

- **Reconstitution Manager**: All organizations must appoint a Reconstitution Manager, who is responsible for planning, managing, and reporting on the recovery of the organization. Additionally, the Reconstitution Manager directs and leads the organization's reconstitution team during all phases of reconstitution, making recommendations to leadership on COAs and serving as the primary point of contact between the organization and the Executive Branch Reconstitution (EBR) Cell. Due to the nature of these duties, it is recommended that the Reconstitution Manager not hold the same responsibilities as those in other continuity personnel roles.

- **Reconstitution Teams**: Planning for reconstitution requires the entire organization's expertise and coordination to ensure a seamless transition back to normal operations. Organizations must identify reconstitution teams with dedicated leadership, staff, and training resources separate from those of the continuity personnel and teams.

8.3. Reconstitution Reporting

Reconstitution Managers at federal organizations generally submit two forms: the GSA Standard Form 2050 (SF-2050) Reconstitution Questionnaire and the Reconstitution Status Report (RSR). The SF-2050 identifies the organization's facility requirements for normal operations prior to a disruption to normal operations. The RSR provides a damage assessment and subsequent repair status update following a disruptive event.

8.3.1. STANDARD FORM 2050

Federal Executive Branch organizations that require GSA for assistance must report reconstitution requirements to GSA. To assist in scoping the federal government's reconstitution plans and programs, organizations with HQ located in the National Capital Region must identify and document anticipated reconstitution needs by annually completing and submitting the SF-2050 Reconstitution Questionnaire.[11] Organizations may contact GSA's Office of Mission Assurance at 202-219-0338 for further instructions.

8.3.2. RECONSTITUTION STATUS REPORT

The RSR is used to report the status of the organization and request assistance from FEMA, OPM, GSA, or NARA. It focuses on three areas: personnel, facilities, and records. The RSR is an invaluable tool for consolidating the information required to determine the organization's reconstitution planning level. The completed RSR lists the location and level of damage to buildings, facilities, and spaces. It captures whether the organization has enough remaining staff following an incident to resume normal operations. The RSR also helps the organization determine the level of damage to records and any accessibility issues.

The RSR provides a real-time view of the organization's reconstitution status during an event. Organizational HQs must submit an RSR, providing the initial, monthly (or as requested), and final status of the organization's reconstitution efforts as it establishes a new normal.

Reconstitution Program Resources

The information provided in this FCD is a brief overview of reconstitution program management requirements. Please see the FEMA *Reconstitution Manager's Guide* for a comprehensive explanation of reconstitution.[12]

For questions regarding reconstitution or assistance with the submission of the RSR, please contact FEMA ONCP at FEMA-NCP-Reconstitution@fema.dhs.gov.

[11] Standard Form 2050 - Reconstitution Questionnaire (gsa.gov)

[12] Reconstitution Manager's Guide | FEMA.gov

This page intentionally left blank

Annex A. Staff and Organization

Federal Executive Branch organizations must identify all continuity personnel in a structure that is organized to support decision-making and the performance of essential functions. Organizations mobilize specific, pre-identified continuity personnel, including management and staff (both government employees and contractor personnel), as necessary to continue to perform essential functions. Continuity personnel can be designated to relocate, be pre-distributed, perform a devolved mission, and/or serve as Out of Area Successors.

Organizations must integrate continuity into all aspects of their mission and across all groups within the organization to improve and increase the resilience of essential functions. All organizational personnel, not just those identified as continuity personnel, should be viewed as resources to perform essential functions in accordance with approved plans and procedures. Continuity programs should include procedures to sustain administrative services, account for personnel, and ensure support services for employees who are not identified as continuity personnel but who are likely to be affected by an emergency.

Organizations must also identify and document orders of succession and delegations of authority to ensure that key personnel can assume key leadership and functional positions as needed. Additionally, the designated personnel must have the appropriate delegated legal authority to make key decisions and take action to ensure the continued performance of essential functions during a disruption to normal operations.

A.1. Roles, Responsibilities, and Integration

Organizations must identify continuity personnel, consisting of leadership and staff who have the operational knowledge, technical expertise, and assets available to perform essential functions at primary sites or alternate sites following relocation, through telework or remote work, or by assuming devolved functions. Decision-makers, Mission Owners, and representatives from across the organization must collaborate with the Continuity Coordinator and Continuity Program Manager to engage with continuity programs, integrate them into the planning process, and be accountable for essential function resilience.

Organizations must identify Emergency Response Group (ERG) and Devolution Emergency Response Group (DERG) members to perform, or ensure the performance of, the organization’s essential functions and services. The ERG is composed of personnel who may relocate from the primary site during a disruption to normal operations. The DERG is composed of alternate individuals predesignated to accept the devolution of authority and responsibility and is geographically separated from the primary site. These groups of continuity personnel may be assisted in these efforts by personnel who have been proactively distributed as a part of normal daily operations and who do not need to transition to devolution or relocation sites to assist in the performance of the organization’s essential functions and services.

Organizations are encouraged to designate other positions to assist in the coordination, implementation, execution, and evaluation of continuity plans and programs. They should ensure that programs incorporate essential functions managed or performed by component or field offices. Organizational continuity roles and responsibilities are further explained in Table 3.

Table 3: Continuity Roles and Responsibilities

Role	*Description*
Leadership	The senior decision-makers who have been elected (e.g., presidents, governors), designated (e.g., cabinet secretaries, administrators), or appointed (e.g., presidentially appointed or Senate confirmed) to head government organizations, including their components. Directors and managers may also serve to guide the organization and make decisions. Leadership must ensure that each part of the organization is involved and accountable in the continuity planning effort. Leaders at the Secretary and Deputy Secretary (or equivalent) levels are required to engage directly to ensure the resilience of essential functions and that National Continuity, including Federal Mission Resilience, remains at the forefront of all intra- and interagency efforts. Senior leaders have the authority to direct such engagement, inform budget priorities, and hold personnel accountable.
Mission Owners	Individuals accountable for performing an essential function that must be sustained during or quickly resumed following a disruption to normal operations. For the Federal Executive Branch, this is the senior accountable government position with the original or delegated authority to lead the Planning, Programming, Budgeting, and Execution (PPBE) and associated risk management of a specific essential function. Mission Owners must integrate continuity into day-to-day operations and empower their personnel to increase the resilience of essential functions.
Continuity Personnel	The leadership, staff, and functional support elements designated to enable the continued performance of essential functions. This includes the Continuity Coordinator; Continuity Program Manager; Out of Area Successor(s); distributed, devolution, and relocation personnel; and other organizational personnel designated to support the continued performance of essential functions.
ERG	Designated continuity personnel who may physically relocate to and continue the performance of essential functions at an alternate site if their primary operating facility or facilities are impacted by a disruption.
DERG	Continuity personnel stationed at a geographically distant site, not the primary site, who are identified to accept the devolution of authority and responsibility for the performance of essential functions.
Distributed Personnel	Personnel who have been proactively distributed as a part of normal daily operations and who do not need to transition to devolution or relocation sites to assist in the performance of the organization's essential functions.

A.2. Orders of Succession

Succession establishes the formal, sequential assumption of a position's authorities and responsibilities, to the extent not otherwise limited by the law, by the holder of another specified position identified in executive order or other presidential directive or in statute, or by relevant organizational policy or regulation if there is no applicable executive order or other presidential directive or statute, in the event of a vacancy in office or a position holder dies, resigns, or is otherwise unable to perform the functions and duties of the pertinent position.

> **Out of Area Successor**: Designated individuals with decision-making authority who are geographically dispersed from the organization's headquarters (HQ) and other individuals within the order of succession. The Out of Area Successor assumes a leadership position if HQ-based personnel are unavailable.

Orders of succession are formal and sequential listings of positions (rather than specific names of individuals) that identify who is authorized to assume a particular leadership or management role under specific circumstances. This is done to support the continuation of organizational command and control and/or the continued performance of essential functions. By including geographically dispersed leaders at regional or field offices in orders of succession, organizations may leverage the advantages of geographic dispersion to ensure that roles and responsibilities are effectively transferred during disruptions to normal operations.

In some cases, organizations may have the latitude to develop orders of succession as they deem appropriate, while in other cases, succession is prescribed by statute, order, or directive. Organizational orders of succession must comply with the Vacancies Reform Act of 1998 (VRA), as amended (5 United States Code [U.S.C.] §§ 3345–3349d), for all presidential appointments that are subject to confirmation by the U.S. Senate. The VRA prescribes conditions regarding the filling of federal vacancies to authorize the President, if an appointed officer of an executive agency (defined to include the Executive Office of the President and exclude the U.S. Government Accountability Office) "dies, resigns, or is otherwise unable to perform office functions, to direct a person who serves in an office for which appointment is required to perform such functions temporarily in an acting capacity, subject to specified time limitations." Although the focus of the VRA is to limit the duration of acting officials in senior positions of the Federal Executive Branch, it also influences orders of succession. As such, the VRA frequently comes into play during disruptions to normal operations.

Organizations and subcomponents must establish and document, in writing, orders of succession in advance of a disruption to normal operations and, in accordance with applicable laws, ensure there is an orderly and predefined transition of leadership during any change in normal operations. Orders of succession can include, but are not limited to, administrators, directors, regional or field directors, and key managers. Organizations are encouraged to have orders of succession reviewed by the General Counsel or equivalent to ensure legal sufficiency. The General Counsel can also address legal issues related to the rules and procedures delegated officials must follow regarding succession;

the conditions under which succession should occur; the method of notification; and any circumstantial, geographic, or organizational limits. Organizations must revise orders of succession as necessary and distribute the revisions promptly to all organizational leadership, Continuity Coordinators, and Continuity Program Managers.

A.2.1. REQUIREMENTS AND CRITERIA FOR ORDERS OF SUCCESSION

Organizations must identify and document orders of succession to ensure that the organization has identified key personnel to assume functional leadership positions if personnel are unavailable.

- Organizations must establish an order of succession to ensure that a designated official is available to serve as acting Organization Head until an official is appointed by the President or other appropriate authority, replaced by the permanently appointed official, or otherwise relieved of the duty of serving as acting Organization Head.
- These orders of succession must comply with the VRA, as amended (5 U.S.C. §§ 3345–3349d).
- Within each order of succession, organizations must include a minimum of three positions (rather than names) permitted to succeed the identified leadership position.
- Orders of succession must outline a process and the criteria to activate procedures for the transition of successors.
- Procedures must be established for notifying appropriate personnel when succession is implemented.
- Organizations must include orders of succession in their essential records and ensure they are accessible at all alternate sites.
- Orders of succession must be reviewed and updated periodically.
- Heads of Category I and II HQ departments and agencies (D/As), as identified in Presidential Policy Directive 40 (PPD-40), *National Continuity Policy*, must include in their orders of succession at least one individual who is geographically dispersed from the Organization Head and other individuals, when possible. Orders of succession for key positions must include an individual who is geographically dispersed relative to identified threats in all categories of HQ and non-HQ orders of succession, when possible.

A.3. Delegations of Authority

Delegations of authority ensure the orderly and predetermined transition of responsibilities within the organization during a continuity activation and are closely tied to succession. They are an essential part of the organization’s continuity program and should have sufficient breadth to ensure that the organization can both continue to maintain command and control as well as perform essential functions. A written delegation of authority provides successors with the legal authorization 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 include restrictions and limitations associated with the authority.

Organizations are encouraged to identify delegations by position title and not by name. However, since many delegations require specific training, qualifications, and certification, organizations may have to associate some delegations of authority with specific individuals (e.g., delegations for committing funds, contracting, technical direction, and classification authority). Delegations of authority outline the conditions under which delegated authority takes effect and the termination process for when authorities are reestablished. Organizations must include written delegations of authority as an essential record and ensure they are available at all alternate sites.

A.3.1. REQUIREMENTS AND CRITERIA FOR DELEGATIONS OF AUTHORITY

In accordance with applicable laws, organizations and subcomponents must establish and document, in writing, the legal authority for the position of the Organization Head and other key leadership positions.

- This document provides the following details for officials to make key decisions during a disruption to normal operations:
  - The explicit authority—including any exceptions to that authority—of an official so designated to exercise organizational direction;
  - The authority of officials to re-delegate functions and activities, as appropriate;
  - The circumstances leading to the delegations of authority taking effect and being terminated;
  - The conditions under which delegations would take place, including the method of notification and the duration of the delegations; and
  - The limitations to the authorities granted by the orders of succession or delegations of authority, including the ability to re-delegate authority.
- Officials listed in the delegations of authority must be informed, in writing, about who might be expected to assume authority in a continuity activation.
- Procedures must be established for notifying appropriate personnel upon implementation of the delegation of authority.
- Delegations of authority must be reviewed and updated periodically.
- The development and revision of delegations of authority must be coordinated with the General Counsel to ensure legal sufficiency.

A.4. Organizational Personnel

Organizations are responsible for utilizing and supporting non-continuity personnel who may be affected by a continuity activation. They should address expectations for non-continuity personnel in continuity plans and/or procedures as well as in emergency plans such as an Occupant Emergency Plan (OEP). Organizations must have the means and process in place to contact and account for employees, and they must communicate this process to all employees.

Organizations must facilitate dialogue among their head of Human Resources, Telework Managing Officer, and Continuity Program Manager when developing continuity plans and programs. Topics to be addressed include the designation of employees who are deemed critical and who must report to the continuity facility, those who are telework-capable to support continuity operations, and those who will be excused from duty due to the emergency (i.e., those who have not been designated as critical employees).

Each Organization Head, or designee, has the authority and responsibility to identify and designate those personnel considered to be critical to the organization's operations during any change in normal operating status, such as a continuity activation, OEP activation, or closure procedures that prevent employees from reporting to their normal operating facility.

Organizations must provide guidance to continuity personnel and all other staff in preparing for, planning for, and staying informed during an emergency. This includes how to procure drive-away and supply kits,[13] create a family emergency plan,[14] and stay informed about different types of emergencies and appropriate responses.[15]

Disaster Preparedness Community Webpage

Organizations should refer to the FEMA Disaster Preparedness Community webpage for additional guidance and resources on how individuals can prepare for disasters.[16]

A.4.1. REQUIREMENTS AND CRITERIA FOR PERSONNEL

Continuity Coordinators are responsible for ensuring that organizational personnel, both continuity and non-continuity, are identified. These personnel must also be listed on a roster that is regularly maintained. Organizations must:

- Develop and implement processes to identify, document, and prepare continuity personnel to conduct or support continuity operations.
- Define the expectations, roles, and responsibilities of continuity personnel.
- Inform continuity personnel and alternates in writing of their continuity roles and responsibilities. Organizations must also obtain a signed acceptance of these roles and responsibilities. See the sample memorandum, "Appointment as an Emergency Response Group Member."
- Maintain a roster of trained personnel capable of performing continuity operations. The roster should include not only primary personnel but also a sufficient number of alternates or backup personnel. Rosters must be reviewed and updated periodically and include, at a minimum, names and office and government-issued cell telephone numbers.

[13] How to Build a Kit for Emergencies | FEMA.gov

[14] Have an Emergency Plan for Your Family | FEMA.gov

[15] Build a Kit | Ready.gov

[16] Preparedness Community Home | FEMA.gov

- If bargaining unit employees are included as continuity personnel, ensure that all applicable collective bargaining obligations are satisfied.
- Develop a strategy and plan for using and supporting non-continuity personnel during continuity activations.
- Provide the ability to communicate with and coordinate activities with non-continuity personnel.
- Provide guidance on the roles and responsibilities of non-continuity personnel. Organizations must communicate how and the extent to which non-continuity personnel are expected to remain in contact with the organization.
- Develop and communicate procedures for how the organization will account for personnel in the affected area during a disruption to normal operations.
- Account for continuity personnel no later than 12 hours after activation.
- Account for all employees in the affected area within five days after the activation of the organization’s continuity plan.
- Implement a process to communicate the organization’s operating status to all staff and stakeholders (e.g., telephone hotline, website, radio or TV broadcast, email).
- Implement a process to contact all staff, including contractors, in the event of an emergency in the affected area.
- Establish procedures and provide the ability to communicate and coordinate activities, including alerts and notifications, with all affected parties. This includes personnel, continuity sites, support teams, and entities with which the affected organization interacts (other organizations, customers, and stakeholders) before, during, and after a disruption to normal operations.
- Communicate how and the extent to which employees are expected to remain in contact with the organization during any emergency.
- Develop and implement a process to communicate to all staff guidance on pay, leave, staffing, and other human resources matters.
- Provide information, provisions, and procedures to assist disaster survivors with special human resources concerns following a disruption to normal operations.
- Establish and maintain procedures to provide guidance to non-continuity personnel.
- Coordinate in advance with labor unions to develop and come to an agreement on procedures that affect union employees.
- Obtain, as an official record, a signed acceptance of these roles and responsibilities.

A.4.2. SAMPLE MEMORANDUM

TO: [Name of ERG Member]

FROM: [Supervisor Name, Office]

SUBJECT: Appointment as an Emergency Response Group Member

You have been identified as critical to agency operations in an emergency. You are hereby appointed as an Emergency Response Group (ERG) member for [Office Name]. ERG members are select personnel assigned to perform essential functions when such functions can no longer be supported from the [Primary/Other] facility due to a local, regional, or national change in operating status and the need to operate from an alternate operating facility exists. If designated to deploy, you must relocate to the alternate site(s). If not designated to deploy, you will remain at your distributed site. In either case, you must establish an operational capability and perform essential functions within 12 hours of a continuity activation.

In a continuity activation, you [will/will not] deploy to [Alternate Site]. Deployment to the alternate site may last for up to 30 days after an event or until normal operations can be resumed.

Respective department heads select each ERG based on the following:

- The identification of predetermined essential functions that must be performed, regardless of the operational status of the [primary/other] building;
- The employee's knowledge and expertise in performing these essential functions;
- The employee's ability to rapidly deploy to the alternate site in an emergency; and
- The employee's ability to be precluded from other emergency assignments.

I understand and accept my assignment as an ERG member for [Office Name] as outlined above.

Signature of ERG member *Date*

This page intentionally left blank

Annex B. Equipment and Systems

Successful performance of essential functions is dependent on the availability of and access to equipment and communications with sufficient resilience and contingencies necessary to perform operations at primary, alternate, devolution, and distributed sites. Organizations must be able to identify and acquire needed equipment during a disruption to normal operations. They must also ensure that equipment and communications systems are compliant with relevant standards and regularly tested to ensure proper functionality during a disruption to normal operations.

B.1. Equipment and Resources

Disasters can disrupt the supply chain, and organizations may need to quickly reestablish access to resources (water, food, pharmaceuticals, medical goods, fuel, etc.). When there has been catastrophic damage to critical infrastructure, such as the electrical grid and telecommunications systems, there will be an urgent need to resume, and possibly redirect, the supply chain and emergency resources. Organizations must plan for supply chain disruptions and pre-position needed resources to ensure the continued performance of essential functions.

Supply Chain Resilience Guide

The Department of Homeland Security (DHS) has developed the *Supply Chain Resilience Guide*, which provides emergency managers with recommendations on how to analyze supply chains and work to enhance supply chain resilience.[17] It also identifies how the results of the supply chain resilience process can inform logistics planning.

B.1.1. EMERGENCY ACQUISITION

The Office of Management and Budget's (OMB) guide *Emergency Acquisitions* assists the federal contracting community with planning and procurement during contingency operations, defense, or recovery from certain attacks, major disaster declarations, or other emergencies.[18] Each emergency is different. Viable readiness plans and personnel trained in emergency contracting procedures will help to optimize the government's responsiveness during a disruption to normal operations. This document highlights pre-emergency planning, considerations when awarding or administering contracts supporting emergencies, and acquisition flexibilities to improve the agility of the acquisition workforce during these critical situations.

[17] Supply Chain Resilience Guide (fema.gov)

[18] Emergency Acquisitions (archives.gov)

The General Services Administration's (GSA) Emergency Acquisition Basic Ordering Agreements offer federal agencies and all levels of government a rapid procurement and delivery mechanism for commercial supplies and services in times of emergency.[19]

B.2. Communications

Communications provide the connection between and among key governmental leadership, internal stakeholders, other organizations, and the public to perform essential functions. Availability, diversity, and redundancy of critical communications are necessary to continue performing essential functions at primary, alternate, distributed, devolution, and telework/remote work sites.

B.2.1. PRIMARY, ALTERNATE, CONTINGENCY, EMERGENCY COMMUNICATIONS

Primary, Alternate, Contingency, Emergency (PACE) communications planning is used to mitigate risk and enhance resilience by developing several fallback plans that ensure the secure emergency communications needed to perform essential functions. It designates the order in which the organization or element will move through available communications systems until contact can be established with the desired distant element. All personnel required to operate essential equipment and systems must be properly trained in and understand the PACE methodology.

- **Primary**: The most common method of communication between parties. Examples include public switched telephone networks, local area networks, and the internet.
- **Alternate**: Another common, but less optimal, method of accomplishing the task. It is often monitored concurrently with primary means. One example is a mobile telephone with both voice and data.
- **Contingency**: This method will not be as fast, easy, inexpensive, or convenient as the first two methods, but it can accomplish the task. Without pre-coordination, however, the receiver rarely monitors this method. One example is a satellite telephone with both voice and data.
- **Emergency**: A method of last resort that typically has significant delays, costs, and/or impacts. It is often monitored only when the other methods fail. One example is a mobile radio system.

[19] Emergency Acquisition Basic Ordering Agreements | GSA

Minimum Requirements for Continuity Communications Capabilities

The Office of Science and Technology Policy (OSTP)/OMB Directive D-16-1, *Minimum Requirements for Federal Executive Branch Continuity Communications Capabilities*, establishes the minimum federal interagency communications requirements for some Federal Executive Branch organizational HQ and alternate sites to enable Federal Executive Branch agency heads, senior leadership, and staff to collaborate, develop policy recommendations, and direct the performance of essential functions under all conditions.

As outlined in the Cybersecurity and Infrastructure Security Agency's (CISA) *Resilient Power Best Practices*, Federal Executive Branch organizations should maintain a diverse set of communications capabilities, which can also make up different components within a PACE planning model (e.g., cellular, satellite, landline, and high frequency [HF] radio).[20] These capabilities should be routinely tested and updated to ensure communications operability and resilience during emergencies.

B.2.2. PRIORITY TELECOMMUNICATIONS SERVICES

CISA provides end-to-end communications priority via three services: Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and Telecommunications Service Priority (TSP).[21]

- GETS is a White House–directed emergency telephone service that provides subscribers with priority access and prioritized processing in the local and long-distance segments of landline telephone networks. Subscribers are issued a personal identification number (PIN) that assigns priority status to calls in service provider networks when used.
- WPS provides authorized devices with priority calling on all nationwide and several regional cellular networks.
- TSP is a CISA-managed Federal Communications Commission (FCC) program. It mandates that service providers prioritize voice and data circuit provisioning and restoration requests made by organizations with national security and emergency preparedness missions.

Organizations must request TSP restoration priority on circuits associated with essential functions before a service outage occurs. They must also pre-position at least one GETS card for emergency use at all primary and alternate sites, issue GETS cards to all continuity personnel, and test GETS and WPS regularly.

[20] Fact Sheet for Resilient Power Best Practices CISA

[21] For additional information on these services, see Priority Services | Cybersecurity and Infrastructure Security Agency CISA.

National Emergency Communications Plan

As the Nation's strategic plan for emergency communications, the *National Emergency Communications Plan* (NECP) establishes a vision to enable the Nation's emergency response community to communicate and share information securely across communications technologies in real time.[22] This includes all levels of government, jurisdictions, disciplines, organizations, and citizens impacted by any threats or hazard events. To achieve this vision, the NECP outlines six nationwide goals and 19 objectives to improve critical capabilities through partnerships, joint planning, and unified investments across levels of government. Its focus is to ensure that the public safety community and citizens are collectively driving toward a common end state for communications.

B.2.3. HIGH VALUE ASSETS

High Value Assets (HVAs) are information or an information system that is so critical to the organization that the loss or corruption of this information or loss of access to the system would have a serious impact on the organization's ability to perform its mission or conduct business. To address the significant vulnerabilities of HVAs, organizations should identify, categorize, and develop an assessment approach to identifying risks and mitigating weaknesses.

Pursuant to the Federal Information Security Modernization Act of 2014 (FISMA),[23] DHS develops and oversees the implementation of Binding Operational Directives (BODs). A BOD is a compulsory direction to Federal Executive Branch organizations for safeguarding federal information and information systems. HVAs can be classified or unclassified. Consistent with DHS BOD 18-02, *Securing High Value Assets*,[24] all Federal Executive Branch organizations are required to report only their non-national security HVAs to DHS. Agency HVA lists must be compliant with OMB M-19-03*, Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*,[25] its successor, or other selection criteria defined by OMB.

B.2.4. OVERVIEW OF CYBER ASSETS AND INCIDENTS

Cyber assets include hardware, software, and networks. Hardware performs the physical functions, software directs and controls the hardware, and networks connect computers, enabling them to communicate and share information. Cyber assets range from systems with local networks to assets with internet access, including smartphones, security systems, building management systems,

[22] National Emergency Communications Plan (cisa.gov)

[23] Public Law 113-283 (congress.gov)

[24] Binding Operational Directive 18-02 | CISA

[25] OMB M-19-03, Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program

heating and air conditioning systems, phone systems, smart home devices, vehicle control systems, and more. By identifying essential functions and understanding how those functions depend on different types of cyber assets, organizations can assess how different types of incidents might affect their key functions. Impacts will often cascade; a disruption to an upstream system can affect any system downstream.

The following is an overview of three common types of cyber incidents. Although each is described independently, any of these incident types is likely to cause overlapping and cascading effects. The compromise of any hardware, software, or network is likely to result in the loss or degradation of services and may allow unauthorized access to confidential information or system controls.

- **Hardware destruction or loss:** The organization's critical services often depend on the hardware (e.g., computers, industrial control systems, storage devices, network infrastructure) that performs critical functions.
- **Network unavailability, compromise, degradation, or destruction:** Networks enable computers to communicate and share information. Most critical services rely on networks. Incidents affecting networks may occur because of both natural disasters and malicious attacks. Since many systems depend on external organizations and are often provided by third parties, an incident affecting the jurisdiction may be the result of a third party's incident.
- **Software malfunction, compromise, or exploitation:** Incidents affecting software may cause the loss or compromise of critical functions. Most of these incidents stem from human error or accidental misconfigurations, but they may also result from malicious attacks.

Continuity personnel should coordinate with cybersecurity/information technology (IT) personnel to regularly review organizational threats and destructive exploits against critical infrastructure. FEMA, in coordination with CISA, released *Planning Considerations for Cyber Incidents: Guidance for Emergency Managers* to help organizations plan for the consequences of a cyber incident.[26] Staff should also review CISA's Shields Up campaign webpage, which provides recommendations, products, and resources to increase organizational vigilance and keep stakeholders informed about cybersecurity threats and mitigation techniques.[27] The complementary Shields Ready campaign webpage provides guidance for critical infrastructure organizations to identify assets and map dependencies, develop plans and exercise capabilities, and implement program evaluation and improvement activities to reinforce readiness.[28]

[26] Planning Considerations for Cyber Incidents: Guidance for Emergency Managers | CISA

[27] Shields Up: Guidance for Organizations | Cybersecurity and Infrastructure Security Agency (cisa.gov)

[28] Shields Ready | Cybersecurity and Infrastructure Security Agency (cisa.gov)

This page intentionally left blank

Annex C. Information and Data

The information and data needed to ensure the continued performance of essential functions must be pre-identified, protected, and backed up. These essential records may be in the form of hard copies or in electronic format, stored on systems and networks. Organizations must have appropriate policies, authorities, and procedures that outline how essential records will be identified and protected, and they must review them annually to ensure that essential records are safeguarded and readily available.

C.1. Information and Data Security

Planning is important to effectively prepare for and respond to a disruptive cyber incident. These incidents may be the result of human error, malicious activity, equipment failure, or a natural disaster. Regardless of their origin, the potential damage to usable information and data may be far-reaching and cascading, requiring continuity personnel to work with cyber incident teams within the organization and beyond.

Planning for such events is generally led by the organization’s Chief Information Officers, who ensure compliance with Federal Information Security Management Act (FISMA) information security requirements. These staff may leverage publications such as the National Institute of Standards and Technology’s (NIST) *Contingency Planning Guide for Federal Information Systems*[29] and *Security and Privacy Controls for Federal Information Systems and Organizations*[30] to inform data protection standards and measures. Continuity personnel may also use the FEMA *Planning Considerations for Cyber Incidents: Guidance for Emergency Managers*, developed in coordination with the Cybersecurity and Infrastructure Security Agency (CISA), to help plan for the consequences of a cyber incident.[31] Additionally, CISA works with each organization to promote the adoption of common policies and best practices that are risk-based and effective for responding to the pace of ever-changing threats.[32]

Organizations must implement preventive activities to protect information and data and mitigate the effects of cyber incidents. Adequate planning based on risk assessments can lessen the impact of incidents, minimize loss and destruction of data, minimize exploits, and return information technology (IT) services to normal. Continuity Program Managers and Mission Owners should work with cybersecurity staff to integrate planning considerations identified in IT/disaster recovery (IT/DR) plans, as appropriate. While information security contingency planning is often unique to each system, it provides preventive measures, recovery strategies, and technical considerations

[29] Contingency Planning Guide for Federal Information Systems | CSRC (nist.gov)

[30] Security and Privacy Controls for Information Systems and Organizations (nist.gov)

[31] Planning Considerations for Cyber Incidents: Guidance for Emergency Managers | CISA

[32] National Cybersecurity Protection System | CISA

appropriate for the system's levels of information confidentiality, integrity, availability requirements, and impact.

Information Technology/Disaster Recovery Plans

It is a common misconception that IT/DR plans are synonymous with or a substitute for a continuity plan. IT/DR plans complement continuity plans, and the two plans should be coordinated. However, an IT/DR plan does not account for how the organization will continue performing its essential functions during a disruption to normal operations. The IT/DR plan impacts the organization's continuity plans and operations by identifying recovery time objectives for key systems that support the performance of functions, including essential functions.

Per FISMA, organizations must provide security for the information and information systems that support operations and assets, including those provided or managed by another organization, contractor, or other source. These systems may host critical information and data that directly support the resilience of the organization's essential functions. Redundant data management software applications and equipment should be standardized throughout the organization and must provide the appropriate controls to protect classified, sensitive, and personally identifiable information.

Access to information (data in a usable form) and data (a set of values that presents facts, concepts, or instructions in a formalized manner) is critical to the continued performance of the organization's essential functions. Organizational Continuity Program Managers and Mission Owners should ensure that essential function continuity planning is integrated into and informs information and data contingency and resilience planning efforts, as well as risk acceptance levels and/or mitigation strategies.

C.1.2. REQUIREMENTS AND CRITERIA FOR INFORMATION AND DATA SECURITY

Organizations must implement preventive activities to protect information and data and mitigate the effects of cyber incidents. Adequate planning based on risk assessments can lessen the impact of incidents, minimize loss and destruction of data, minimize exploits, and return IT services to normal.

- Organizations must provide security for the information and information systems that support operations and assets, including those provided or managed by another organization, contractor, or other source.
- Continuity Program Managers and Mission Owners should:
  - Ensure that essential function continuity planning is integrated into and informs information and data contingency and resilience planning efforts; and
  - Work with cybersecurity staff to integrate planning considerations identified in IT/DR plans, as appropriate.

C.2. Essential Records

Essential records are those records the organization needs to meet operational responsibilities during national security emergencies or other emergencies (*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*).

In addition to originals or copies of essential records—regardless of their format—organizations must consider the protection and use of complementary information systems, technology, applications, infrastructure, and references needed to support the continued performance of essential functions and continuity operations during an activation. Organizations must establish an essential records program for the identification, protection, and availability of electronic and hard copy essential records, as well as the electronic information systems needed to support essential functions during all-hazards emergencies.

Organizations must protect the information needed to resume normal operations for reconstitution. Each organization has different functional responsibilities and business needs. The organization decides which records are essential to its operations and then assigns appropriate personnel the responsibility for maintaining current copies of those records. Organizations should have multiple copies of their essential records in several locations stored on redundant media and in virtual storage environments.

Categories of essential records include the following:

- **Emergency Operating Records:** Records and electronic information systems essential to the continued functioning or reconstitution of the organization during and after a continuity activation. Examples of these types of records are emergency plans and directives, orders of succession, delegations of authority, staffing assignments, and related policy or procedural records. These records provide the organization's continuity personnel with the guidance they need to continue and resume normal operations.

- **Legal and Financial Rights Records:** Records that are critical to carrying out the organization's essential legal and financial functions and vital to the protection of the legal and financial rights of individuals who are directly affected by that organization's activities. These records include those with such value that their loss would significantly impair the performance of essential functions and the legal or financial rights and entitlements of the organization and the affected individual(s). Examples of these records are accounts receivable files; contracting and acquisition files; official personnel records; Social Security, payroll, retirement, and insurance records; and property management and inventory records. Legal and financial rights records considered critical for the continued performance of essential functions and continuity operations should be included in emergency operating records and accessible at the appropriate continuity facility.

The National Archives and Records Administration (NARA) provides information on essential records regulations and recommended practices to develop and implement federal records disaster mitigation and records recovery programs. Federal agencies may find NARA's essential records checklist useful in evaluating their records management procedures for essential records.[33]

C.2.1. ESSENTIAL RECORDS PLAN

Organizations must develop an essential records plan to document all aspects of the essential records program. The essential records plan must include an inventory of and access instructions for all emergency plans, including the continuity plan and related records that detail the organization's response to an emergency. Organizations must include instructions for moving essential records from the primary site to the alternate site, if necessary, in both the continuity plan and the essential records plan. Although some organizations may elect to maintain all essential records in an electronic format, the essential records plan should detail alternative methods for accessing records, such as on-site hard copies. Organizations should identify an Essential Records Manager who will be primarily responsible for essential records management tasks.

C.2.2. REQUIREMENTS AND CRITERIA FOR ESSENTIAL RECORDS MANAGEMENT

Organizations must develop an essential records plan to document all aspects of the essential records program.

- An official essential records program must:
  - Identify and protect those records that specify how the organization will operate in an emergency or disaster, including appropriate policies, authorities, and procedures;
  - Identify and protect those records needed to protect the legal and financial rights of the government and citizens;
  - Identify and protect those records necessary to the organization's continuity operations, including the performance of essential functions and the reconstitution of normal operations; and
  - Include the written designation of an Essential Records Manager and the assignment of responsibilities to specifically designated staff.
- Continuity personnel must have appropriate access at alternate sites to the required media (e.g., paper, photographic film, microform and/or electronic forms), equipment, and instructions for retrieving essential records, including, but not limited to, records stored in cloud-based applications and accessed via the internet or a virtual private network.

[33] Essential Records Guide (archives.gov)

- Organizations must conduct an essential records risk assessment at least annually to accomplish the following:

    - Identify the risks associated with retaining essential records in their current locations and determine the difficulty of reconstituting the records if destroyed;
    - Identify off-site storage locations and requirements;
    - Ensure that all appropriate storage methods and formats are used;
    - Determine the requirements to provide alternate storage locations for duplicate records to guarantee the ready availability of essential records under all conditions and address the capture and protection of work-in-progress essential information; and
    - Document the date of the review and, at minimum, the name, position title, and contact information of the senior-most person and an alternate who conducted the review.

- Based on risk assessment results, organizations must implement needed protections for essential records. This includes dispersing those records to other organizational locations or storing those records off-site or electronically in an automated system. When determining and selecting protection methods, it is important to consider the special equipment, hardware, software, and access rights or permissions needed for each type of storage system or media.

- Organizations must develop and maintain an essential records packet and include a copy of the packet at alternate sites. An essential records packet is an electronic or hard copy compilation of key information, instructions, and supporting documentation needed to access essential records during an emergency. Packets should be updated on the same schedule as all other essential information so that they remain current.

- An essential records packet must include the following:

    - An electronic and/or hard copy list of leadership, Mission Owners, and continuity personnel (such as Emergency Response Group [ERG], Devolution Emergency Response Group [DERG], and Out of Area Successors) with up-to-date telephone numbers;
    - An inventory of essential records with the precise locations for these records;
    - Information about how to obtain the necessary access mechanisms (e.g., keys, access readers);
    - Alternate site information;
    - Access requirements and lists of equipment sources necessary to access the records (e.g., hardware and software, file storage and synchronization services, microform/microfilm readers, internet access, dedicated telephone lines);
    - Lists of record recovery experts and vendors; and
    - A copy of the organization's continuity plans.

- Organizations must annually review their essential records program to address new security issues, identify problem areas, and update information to ensure that the latest versions are available. They must also document the date of the review and, at minimum, the name, position title, and contact information of the senior-most person and an alternate who conducted this review.

- Identify any missing essential records that are required for the organization to perform its essential functions.
- Incorporate into the program additional essential records generated by program, function, or organizational change to existing programs or functions.
- Remove records from the essential records inventory and storage locations when they are superseded or are no longer applicable according to the records retention schedule or the NARA-issued General Records Schedules (GRS 4.1).

Annex D. Sites

Primary sites are where organizations perform the day-to-day operations of either or both their essential functions and command and control. Organizations must identify alternate sites that are unlikely to be affected by the same incident that disrupts those functions at the primary site. At these alternate sites, personnel must have access to the equipment, systems, software, information, and data needed to perform essential functions until the organization can reconstitute at a repaired or new facility.

All Federal Executive Branch organizations must be able to conduct essential functions and services from an alternate site, whether through distribution, devolution, or relocation. A devolution site is a facility outside the region of the primary facility that is used to perform essential functions and is staffed by the Devolution Emergency Response Group (DERG). In some cases, operations cannot be physically devolved or relocated but must be hardened.

While relocation and hardening remain valid continuity options to mitigate many threats and hazards, organizations are encouraged to distribute operations. Distribution complements devolution, relocation, and hardening. Distributing operations, along with reducing single points of failure, requires the use of scalable, flexible, and adaptable operations techniques across dispersed geographic areas.

The organization's ability to distribute its regular operations across geographically separate sites that are less likely to be affected by the same disruption increases the likelihood that it can successfully continue performing its essential functions under any conditions. In addition to hardened infrastructure, devolution and relocation capabilities support and complement distributed operations by providing leaders with more choices for personnel and locations to continue performing essential functions.

The organization may use one or a combination of continuity options—such as distribution, devolution, relocation, or hardening—to ensure the performance of its essential functions. Telework may be used to provide additional flexibility and augment the performance of essential functions, but due to its voluntary nature and potential risks of communications and power outages, it should not be the organization's sole or primary continuity option.

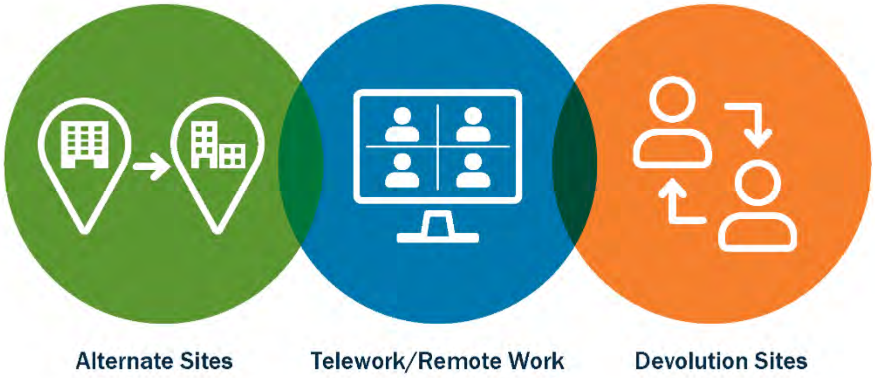


Figure 7: Continuity Options Flexibility

D.1. Alternate Sites

Alternate sites refer to facilities where the performance of essential functions continues or resumes and where organizations maintain command and control of essential functions during a disruption to normal operations. Organizations must have physical alternate sites, as determined by their risk assessment, to continue performing essential functions. An alternate site is a facility within the same region, sufficiently distant from the primary facility, that is used to conduct continuity operations and is staffed by deployed Emergency Response Group (ERG) members.

Organizations must consider sites that are not uniquely susceptible to risks associated with natural disasters. The facilities at these sites must have access to power, telecommunication services, and the internet that are separate from the grids of the primary facility, whenever possible. Organizations should identify alternate sites that would not be affected by the same disruption to normal operations that is driving operations away from the primary site. Selection should be based on the general principle of proximity—in other words, away from the organization's primary site.

Organizations should consider maintaining multiple sites for varying levels of risk and severity of threat. For example, the organization may select an alternate site in the immediate geographic location as its primary site for use in the event of a burst pipe or fire in the main building. Organizations must also maintain alternate sites located farther away for use in situations causing greater damage and reducing the organization's ability to operate locally (e.g., flood, earthquake). Ultimately, the Organization Head is responsible for deciding which alternate sites will be used to ensure the continued performance of the organization's Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs).

When identifying and preparing continuity sites for operation, organizations should maximize the use of existing infrastructure. They should also use technology to enhance the effectiveness of continuity programs through telework, mobile work, and joint or shared facilities.

Alternate sites are categorized in the following three ways:

- **Hot sites:** Sites that operate 24 hours a day with fully operational equipment and the capacity to immediately assume operations upon loss of the primary site. A hot site requires on-site telecommunications, information, infrastructure, equipment, backup data repositories, and personnel to perform essential functions.

- **Warm sites:** Sites that have a minimum acceptable level of infrastructure in place and possess the information technology (IT) and telecommunications equipment to become operational to support the performance of essential functions as soon as possible, but not later than 12 hours after continuity plan activation. These sites may be in use regularly to support some aspects of normal operations. A warm site typically requires additional personnel, equipment, supplies, software, or customization to be fully operational. Warm sites generally have the resources necessary to sustain critical mission/business processes but lack the capacity to activate all systems or components immediately upon a disruption to normal operations.

- **Cold sites:** Sites that are neither staffed nor operational on a daily basis. Telecommunications, IT equipment, and other infrastructure are typically present; however, personnel must be deployed to activate the systems before the site can become operational. Basic infrastructure and environmental controls (e.g., electrical and heating, ventilation, and air conditioning systems) are present, yet systems are not continuously active.

Organizations may use existing space for alternate sites, including:

- **Remote/offsite training facilities:** These sites include training centers located near the organization’s primary facility but with sufficient distance to afford geographic dispersion.

- **Regional or field offices:** Regional or field offices may serve as suitable alternate sites for headquarters (HQ) operations.

- **Remote HQ operations:** Operational HQ locations that occupy geographically dispersed offices may designate one or more of these facilities as alternate sites.

- **Co-location:** The organization may relocate to another organization’s facilities. The relocating organization might occupy available space in the receiving organization’s HQ, training facilities, or field offices. Co-location is often coordinated via reciprocal agreements: each organization agrees to host the other in a contingency that may affect only one of the organizations.

- **Space procured and maintained by the U.S. General Services Administration (GSA):** The organization may enlist the assistance of GSA to acquire, equip, and sustain privately and/or federally owned and leased space to accommodate continuity requirements.

- **Space procured and maintained by another organization:** Some organizations other than GSA offer space procurement services for use by organizations that require an alternate site.

- **Joint-use continuity facilities:** Several organizations may pool resources to acquire a joint continuity facility for use as their alternate site. Organizations must use care to avoid overcommitment of joint-use facilities during continuity activations. Additionally, it is imperative that each organization have designated resources in joint-use facilities.

- **Alternate use of existing facilities:** In certain types of disruptions, organizations may use existing facilities but employ methods, such as social distancing, to support continuity operations. Organizations may also use existing facilities, but in different capacities. For example, a facility normally used for command and control may instead be used to support the performance of essential functions, or if multiple facilities support the performance of a function, activities may be combined at one.

Federal Executive Branch organizations, regardless of geographic location, must identify and document the locations of alternate facilities by completing and submitting the GSA Standard Form 336 (SF-336), Continuity of Operations Alternate Facility Identification/Certification.

- Organizations may download this form from GSA's website to submit their unclassified information.[34]
- Organizations are required to review and submit their SF-336 to GSA annually.
    - Organizations must submit preliminary site documentation by using SF-336 to gain approval before committing resources. The form must be submitted at least 30 days prior to the formal commitment or contract to occupy the facility.
- Organizations with access to classified systems must also register and annually submit their completed forms to GSA via secure methods.
- If the organization no longer requires a facility currently in use, it must notify GSA 30 days prior to vacating the site by submitting an updated SF-336.
- Organizations may contact GSA's Office of Mission Assurance at 202-219-0338 for further instructions.

D.1.1. REQUIREMENTS AND CRITERIA FOR ALTERNATE SITES

Organizations must perform the following actions (at a minimum) to support the deployment of their ERGs:

- Establish and maintain alternate sites for relocation during disruptions to normal operations;
- Review alternate sites for suitability and functionality at least annually, validate continuity requirements, and document the date and names of personnel conducting the review/validation per the organization's internal process;

[34] Standard Form 336 - Continuity of Operations Alternative Facility Identification/Certification (gsa.gov)

- Establish and implement procedures for the reception, processing, and orientation of continuity personnel; and
- Coordinate with site facility managers to ensure the availability of space and services.

Organizations at alternate sites that are neither owned nor leased must have a current, signed memorandum of agreement/memorandum of understanding (MOA/MOU) with the owner or occupant of the facility. They must also review the MOA/MOU annually or following any leadership changes. At a minimum, MOAs/MOUs must specify:

- The amount of time required for the owner/occupant to have the facility configured for occupancy;
- Details of the space and services to be provided at the facility;
- Access control procedures for the allocated space during occupancy; and
- The date of the review and, at minimum, the name, position title, and contact information of the senior-most person and an alternate who conducted the review.

Organizations must ensure that the following capabilities exist at alternate sites prior to activation or will become available as soon as possible but not later than 12 hours after activation:

- The performance of essential functions with minimal disruption of operations for a minimum of 30 days or until normal operations are resumed.
- The replication of essential capabilities by providing systems and configurations that are used in everyday activities.
- Access to and use of essential records necessary to conduct continuity operations.
- Interoperable communications, including secure communications if appropriate, with all identified internal and external stakeholders.
- Up-to-date computer equipment, software, information systems, and other automated data processing equipment necessary to conduct continuity operations.
- Access to essential resources—such as food, water, fuel, medical, and municipal services—to ensure the health, safety, and security of the facility and its personnel.
- Emergency/backup power in case the primary power source is disrupted.
- Lodging to support deployed continuity personnel at or near the facility. This can include lodging within the facility, rooms at private or commercial facilities (e.g., hotels, motels), and/or employee residences if within commuting distance.
- An organization-specific transportation support plan that details navigation information and any en route communication needs the organization decides are necessary for ERG members traveling to, from, and at the physical alternate sites.
- Sufficient levels of security to protect against all threats, as identified in the facility's risk assessment and physical security surveys. This includes sufficient personnel to provide perimeter, access, and internal security, as required by organizational policy.

Organizations must comply with GSA's requirements for completing and submitting the GSA SF-336 Alternate Facility Reporting Form:

- Initial submission of the SF-336 to GSA; and
- Annual review and resubmission of the SF-336 to GSA.

GSA SF-336 Alternate Facility Reporting Form

Federal Executive Branch organizations must identify and document the locations of continuity facilities via the completion and submission of the SF-336 GSA Alternate Facility Reporting Form.[35]

D.2. Telework and Remote Work Flexibility

All organizations must incorporate telework and remote work arrangements into their continuity plans. These arrangements, in combination with devolution and alternate sites, can be part of the organization's broader distribution option to perform essential functions and supporting activities. The Telework Enhancement Act of 2010, which applies to all Federal Executive Branch organizations, authorizes telework procedures to support organizational missions and everyday operations.[36]

Telework can help the organization perform essential functions during a change to its normal operating status (e.g., during a pandemic or a flood that causes a partial building closure). However, due to its vulnerability to power or communications outages, it may not be viable for continuing essential functions during all events (e.g., cyber events, mass power outages) and should not be relied upon as the organization's sole primary option. The reliance on commercial infrastructure presents its own risks and should be considered when including telework as a part of a continuity option.

Organizations must assess each activity, task, or responsibility associated with continuity operations to determine if it can be performed via telework or whether it must be performed, in part or in whole, at an alternate site. This includes:

- Supporting functions or capabilities necessary to ensure the continued performance of essential functions.
- Ensuring the ability to perform essential functions and services in case telework is not viable (e.g., significant power and/or telecommunications infrastructure degradation).

[35] Continuity of Operations (COOP) -- Continuity Facility Identification/Certification | GSA

[36] Telework – OPM.gov

- Identifying employees who are unable to perform designated functions through telework and must therefore perform continuity operations on-site. In the case of an infectious biological incident, for example, the organization must classify the associated risk exposure level for affected employees. It must also inform them in advance that they are expected to work on-site and provide appropriate or necessary administrative controls, training, and/or personal protective equipment.

Organizations must identify and document in their continuity plans which essential functions can be performed via telework. They must also evaluate the use of telework for supporting extended continuity operations and its use by non-ERG personnel. Organizations must establish and maintain plans, policies, and procedures for telework in coordination with the organization's continuity plans. This includes:

- Coordinating with the organization's designated Telework Managing Officer when developing and integrating telework considerations into the organization's continuity plans; and
- Notifying continuity personnel that they are filling positions identified as telework-capable.

Telework arrangements fall into two categories:

- **Routine:** Telework that occurs as part of an ongoing regular schedule such that employees typically telework on identified days and work at their agency worksite on others during each pay period.
- **Situational:** Telework that is approved on a case-by-case basis and the hours worked were not part of a previously approved, ongoing, and regular telework schedule.

Organizations must adhere to Office of Personnel Management (OPM) and internal policy and guidance governing the use of telework and remote work.[37] They must provide for the security of information and information systems during remote work activities according to government standards. They must also provide access to essential records, databases, and the robust communications necessary to perform the organization's essential functions at telework and remote work locations. Organizations should coordinate with their Chief Security and Chief Information Officers to identify equipment and technical and security support requirements for personnel identified as telework- and remote work–capable.

D.3. Devolution Sites

Devolution planning addresses how the organization will identify and transfer organizational command and control, as well as responsibility for performing essential functions, to personnel at a geographically dispersed location unaffected by the incident. Organizations may activate their DERG

[37] For additional guidance on telework/remote work, refer to OPM's website, OPM Home – OPM.gov, and the *2021 Guide to Telework and Remote Work in the Federal Government*, at 2021 Guide to Telework and Remote Work in the Federal Government (opm.gov).

as a short-term continuity option while ERG members relocate to their alternate site(s) or when ERG members are unavailable or unable to perform their roles. Additionally, organizations may choose to partially devolve by transferring responsibilities for select essential functions or devolve to multiple sites by transferring responsibilities for designated essential functions to specific sites.

The devolution counterpart must be able to perform essential functions as soon as possible, but not later than 12 hours after devolution plan activation. It must be able to sustain operations for a minimum of 30 days, or until normal operations are resumed. When selecting a devolution site, organizations must consider the capabilities of the site to ensure it has the communications systems, equipment, and resources pre-positioned or available within the accepted timeframe to enable the organization to assume responsibility for the performance of essential functions.

Table 4: Summary of Continuity Sites

Alternate Sites	Telework/Remote Work Flexibility	Devolution Sites
Alternate sites are fixed, mobile, or transportable sites, other than the primary HQ facility, where organizational continuity personnel relocate in order to perform essential functions and/or maintain command and control following activation of the continuity plan. These locations include sites where telework and mobile work occur. Organizations should consider maintaining one or more sites that are located across dispersed geographic areas and selected based on varying degrees of risk and severity of threat.	**Telework** refers to a flexible work arrangement in which an employee situationally or routinely performs duties and responsibilities from an approved worksite while still reporting to their agency worksite on a regular and recurring basis. **Remote work** is an arrangement in which an employee performs work from an approved worksite but is not expected to report to the agency worksite on a regular and recurring basis. Employees who participate in an approved telework and/or remote work program may be incorporated into the organization's continuity plans and may be leveraged during emergencies.	**Devolution** is a component of continuity planning that establishes procedures to transfer statutory authority and responsibilities from the organization's primary operating staff to other staff to maintain organizational command and control and/or perform essential functions when necessary. Devolution may be temporary or may endure for an extended period. A devolution plan is activated upon the threat of, or in response to, a disruption to normal operations that either renders the organization's primary operating staff unavailable or leaves them incapable of performing essential functions from primary facilities.

Annex E. Authorities and Resources

Authorities

Atomic Energy Act (42 United States Code [U.S.C.] §§ 2011–2259).

Federal Advisory Committee Act, as amended (5 U.S.C. §§ 1001–1014).

Federal Information Security Modernization Act of 2014, Pub. L. No. 113–283, 128 Stat. 3073 (2014).

Homeland Security Act of 2002, as amended (6 U.S.C. § 101 et seq.).

Telework Enhancement Act of 2010 (5 U.S.C. §§ 6501–6506).

Vacancies Reform Act of 1998, as amended (5 U.S.C. §§ 3345–3349d).

Executive Order 12148, *Federal Emergency Management*, July 20, 1979, as amended.

Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities,* Nov. 18, 1988, as amended.

Executive Order 13526, *Classified National Security Information*, Dec. 29, 2009.

Executive Order 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, July 6, 2012.

Presidential Policy Directive 8, *National Preparedness*, March 30, 2011.

Presidential Policy Directive 40, *National Continuity Policy*, July 15, 2016.

National Security Memorandum 22, *Critical Infrastructure Security and Resilience*, April 2024.

National Security Presidential Memorandum 28, *National Operations Security Program*, January 2021.

Federal Mission Resilience Strategy, Dec. 7, 2020.

Resources

36 Code of Federal Regulations, Part 1223, *Managing Vital Records*.

36 Code of Federal Regulations, Part 1236, *Electronic Records Management*.

44 Code of Federal Regulations, Part 3541, *Federal Information Security Management Act of 2002*.

Congressional Research Service, *The Executive Budget Process: An Overview*, May 2022.

Cybersecurity and Infrastructure Security Agency, *CISA Insights: Secure High Value Assets*, [no date].

Cybersecurity and Infrastructure Security Agency, *Fact Sheet for Resilient Power Best Practices*, November 2022.

Cybersecurity and Infrastructure Security Agency, *National Emergency Communications Plan*, September 2019.

Cybersecurity and Infrastructure Security Agency, *National Infrastructure Protection Plan (NIPP)*, 2013.

Cybersecurity and Infrastructure Security Agency, *NIPP Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach*, December 2020.

Cybersecurity and Infrastructure Security Agency, *Planning Considerations for Cyber Incidents: Guidance for Emergency Manager*s, November 2023.

Department of Homeland Security, Binding Operational Directive 18-02, *Securing High Value Assets*, May 2018.

Department of Homeland Security, *Homeland Security Exercise and Evaluation Program (HSEEP)*, January 2020.

Department of Homeland Security, *Supply Chain Resilience*, April 2019.

Department of Homeland Security/Federal Emergency Management Agency, *Department of Homeland Security Federal Emergency Management Agency Security Classification Guide 100.3*, October 2022.

Department of Homeland Security/Federal Emergency Management Agency, FCD-2, *Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process*, June 13, 2017.

Federal Emergency Management Agency, *Executive Branch Reconstitution Concept of Operations*, January 2021.

Federal Emergency Management Agency, *Federal Continuity Directive: Continuity Planning Framework for the Federal Executive Branch*, December 2023.

Federal Emergency Management Agency, *How to Build a Kit for Emergencies*, June 2020.

Federal Emergency Management Agency, Memorandum of Understanding Between the U.S. Office of Personnel Management and the U.S. Department of Homeland Security, August 2008.

Federal Emergency Management Agency, National Continuity Programs, *Executive Branch Reconstitution Concept of Operations*, January 2021.

Federal Emergency Management Agency, National Continuity Programs, *Guide to Continuity Program Management*, May 2010.

Federal Emergency Management Agency, *National Exercise Program Base Plan*, October 2018.

Federal Emergency Management Agency, *National Preparedness Goal*, September 2015.

Federal Emergency Management Agency, *Reconstitution Manager's Guide*, April 2023.

Interagency Security Committee, *The Risk Management Process: An Interagency Security Committee Standard*, 2021.

National Archives and Records Administration, *Essential Records Guide*, August 2018.

National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, September 2020.

National Institute of Standards and Technology, Special Publication 800-30, Rev. 1, *Guide for Conducting Risk Assessments*, September 2012.

National Institute of Standards and Technology, Special Publication 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.

National Institute of Standards and Technology, Special Publication 800-39, *Managing Information Security Risk Organization, Mission, and Information System View*, March 2011.

National Institute of Standards and Technology, Special Publication 800-53, Rev. 4, *Recommended Security Controls for Federal Systems and Organizations*, August 2013.

Office of Management and Budget, Circular No. A–11, *Preparation, Submission, and Execution of the Budget*, August 2023.

Office of Management and Budget, *Emergency Acquisitions*, January 2011.

Office of Management and Budget, Memorandum M-05-16, *Regulation on Maintaining Telecommunication Services during a Crisis or Emergency in Federally-owned Buildings*, June 30, 2005.

Office of Management and Budget, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, December 2018.

Office of Science and Technology Policy/Office of Management and Budget, Directive D-16-1. *Minimum Requirements for Federal Executive Branch Continuity Communication Capabilities,* December 2016, as amended.

Office of the Director of National Intelligence, Intelligence Community Standard Number 500-19, *Universal Access and Remote Access to TS/SCI Web Content and Services*, July 7, 2010.

U.S. Department of the Interior, “Definitions of Insular Area Political Organizations,” Definitions of Insular Area Political Organizations | U.S. Department of the Interior (doi.gov).

U.S. Office of Personnel Management, *2021 Guide to Telework and Remote Work in the Federal Government*, November 2021.

U.S. Office of Personnel Management, *Guide to Telework in the Federal Government*, April 2011.

U.S. Office of Personnel Management, *Handbook on Pay and Leave Benefits for Federal Employees Affected by Severe Weather Conditions or Other Emergency Situations*, June 2008.

U.S. Office of Personnel Management, *Human Resources Flexibilities and Authorities in the Federal Government*, August 2013.

U.S. Office of Personnel Management, “Telework Coordinator,” What Is the Definition of Remote Work? - OPM.gov.

U.S. Office of Personnel Management, *Washington, DC, Area Dismissal and Closure Procedures*, December 2015.

This page intentionally left blank

Annex F. Definitions

Activation – The implementation of a continuity plan, in whole or in part (Source: FEMA).

All-Hazards – A classification encompassing all conditions, environmental or human-caused, that have the potential to cause injury, illness, or death; damage to or loss of equipment, infrastructure services, or property; or alternatively causing functional degradation to social, economic, or environmental aspects. These include accidents, technological events, natural disasters, space weather, domestic and foreign-sponsored terrorist attacks, acts of war, weapons of mass destruction (WMDs), and chemical, biological (including pandemic), radiological, nuclear, or explosive (CBRNE) events (Source: FEMA).

Alternate Sites – Fixed, mobile, or transportable sites, other than the primary headquarters (HQ) site, where organizational continuity personnel relocate to perform essential functions and/or provide command and control following activation of the continuity plan. They include sites where telework and mobile work occur (Source: FEMA).

Business Impact Analysis (BIA) – A method of identifying threats and hazards that may impact the performance of essential functions, along with problem areas such as resource gaps, process weaknesses, consolidated points of failure, and other vulnerabilities (Source: FEMA).

Business Process Analysis (BPA) – A systematic method of examining, identifying, and mapping the processes, continuity planning factors (Staff and Organization, Equipment and Systems, Information and Data, and Sites), and other resources (including budget) needed to perform a Mission Essential Function (MEF) (Source: FEMA).

Catastrophic Emergency – "Any event, regardless of location, that results in extraordinary levels of mass casualties, damage or disruption severely affecting the U.S. population, infrastructure, environment, economy or Government Functions" (Source: Presidential Policy Directive 40 [PPD-40], *National Continuity Policy*).

Category – Refers to the categories of organizations commensurate with their responsibilities during a catastrophic emergency. These categories are used for developing continuity planning, communications and information services requirements, emergency operations capabilities, and other related requirements (Source: PPD-40, *National Continuity Policy*).

Cold Sites – Sites that are neither staffed nor operational on a daily basis. Telecommunications, information technology (IT) equipment, and other infrastructure are typically present; however, personnel must be deployed to activate the systems before the site can become operational. Basic infrastructure and environmental controls (e.g., electrical and heating, ventilation, and air conditioning systems) are present, yet systems are not continuously active (Source: FEMA).

Communications – Voice, video, and data capabilities that enable organizational leadership and staff to ensure the performance of essential functions. Robust communications enable leadership to receive coordinated and integrated policy and operational advice and recommendations. This provides government organizations and the private sector with the ability to communicate internally and with other entities (including other federal organizations; state, local, tribal, and territorial [SLTT] governments; and the private sector) as necessary to perform essential functions (Source: FEMA).

Component – A major subdivision of an organization, separately organized and clearly distinguished in work function and operation from other organizational subdivisions (Source: FEMA).

Continuity – The uninterrupted performance of essential functions before, during, and after an event that disrupts normal operations (Source: FEMA).

Continuity Advisory Group (CAG) – A continuity policy coordination committee focused on interagency implementation of continuity programs. The CAG is comprised of Continuity Coordinators, or their designees, from Category I, II, III, and IV departments and agencies (D/As). Key state and local government representatives from the National Capital Region (NCR) and representatives from the legislative and judicial branches are invited to participate in meetings, as appropriate (Source: FEMA).

Continuity Capability – The ability of an organization to maintain the performance of its essential functions before, during, and after an event that disrupts normal operations (Source: FEMA).

Continuity Coordinator – A senior accountable Federal Executive Branch official at the Assistant Secretary or equivalent level who represents their organization on the CAG, ensures continuity capabilities in the organization, and provides recommendations for continuity policy. Continuity Coordinators are supported primarily by the Continuity Program Manager and by other continuity planners or coordinators at their subordinate levels throughout their organizations (Source: FEMA).

Continuity of Government (COG) – "A coordinated effort within the executive, legislative or judicial branches of the Federal Government to ensure that NEFs [National Essential Functions] continue to be performed during a catastrophic emergency" (Source: PPD-40, *National Continuity Policy*).

Continuity of Operations – "An effort within the Executive Office of the President (EOP) and individual [organizations] to ensure that essential functions continue to be performed during disruption of normal operations" (Source: PPD-40, *National Continuity Policy*).

Continuity Personnel – The leadership, staff, and functional support elements designated to enable the continued performance of essential functions (Source: FEMA).

Continuity Plan – A document that details how an individual organization will ensure it can continue to perform its essential functions during a wide range of events that impact normal operations (Source: FEMA).

Continuity Program Manager – The individual responsible for managing day-to-day continuity programs and reporting to the Continuity Coordinator on all continuity program activities. This person may also be designated to represent the organization on the CAG and other working groups, as appropriate (Source: FEMA).

Continuous Improvement Program (CIP) – An organized method of documenting and tracking improvement actions for an organization's continuity program (Source: FEMA).

Controlled Unclassified Information (CUI) – "Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable laws, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended" (Source: National Archives and Records Administration [NARA]).

Critical Asset – An asset of such strategic importance to the performance of essential functions that its incapacitation or destruction would have a very serious or debilitating effect on the organization's ability to perform the function(s) (Source: FEMA).

Critical Infrastructure – Systems and assets, whether physical or virtual, so vital to the United States that the incapacitation or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or a combination of those matters (Section 1016 of the USA Patriot Act of 2001 [42 U.S. Code (U.S.C.) § 5195c]) (Source: U.S. Code).

Data – A value or set of values that provides a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means (Source: Department of Homeland Security [DHS]).

Departments and Agencies – Those executive departments enumerated in 5 U.S.C. § 101, independent establishments as defined by 5 U.S.C. § 104(1), government corporations as defined by 5 U.S.C. § 103(1), the intelligence community as defined by 50 U.S.C. § 3003, and the U.S. Postal Service (USPS) (Source: U.S. Code). *Note that this document refers to D/As, commissions, bureaus, boards, and independent organizations as "organizations."*

Devolution – The transfer of statutory authority and responsibility from an organization's primary operating staff to other staff to maintain organizational command and control and/or perform essential functions when necessary (Source: FEMA).

Devolution Emergency Response Group (DERG) – Alternate individuals predesignated to accept the devolution of authority and responsibility and geographically separated from the primary site (Source: FEMA).

Directed Work – Work performed at a location at which an employee is directed to work, other than the official worksite. This can be the employee's residence or another approved alternate work location (Source: FEMA).

Disruption – An event that causes an unplanned interruption in operations or functions (Source: FEMA).

Distribution – A continuity option for reducing overall risk to essential functions. This is achieved through dispersing Staff and Organization, Equipment and Systems, Information and Data, and Sites to mitigate vulnerabilities (Source: FEMA).

Drive-Away Kit – A kit prepared by and for an individual who expects to deploy to an alternate location during an emergency. The kit contains items needed to minimally satisfy an individual's personal and professional needs during deployment, such as clothing, medications, a laptop, and other necessities (Source: FEMA).

Emergency Operating Records – Records an organization needs to continue functioning or to reconstitute after an emergency (Source: NARA).

Emergency Plan – Documented procedures that direct coordinated actions to be undertaken in response to threats that are typically of limited duration and do not require an organization to activate its continuity plan. Also referred to as an Occupant Emergency Plan (OEP) or Building Closure Plan (Source: FEMA).

Emergency Response Group (ERG) – Designated continuity personnel who may physically relocate and continue the performance of essential functions at an alternate site (Source: FEMA).

Enduring Constitutional Government (ECG) – "A cooperative effort among the executive, legislative and judicial branches of the Federal Government, coordinated by the President, as a matter of comity to the legislative and judicial branches and the constitutional separation of powers among the branches, to preserve the constitutional framework under which the Nation is governed. ECG includes the capability of all three branches of government to execute constitutional responsibilities and provide for orderly succession, appropriate transition of leadership, and interoperability and support of the NEFs during a catastrophic emergency" (Source: PPD-40, *National Continuity Policy*).

Essential Functions – "Subsets of Government Functions that are categorized as MEFs, PMEFs [Primary Mission Essential Functions] and NEFs" (Source: PPD-40, *National Continuity Policy*).

Essential Records – Records (emergency operating records) to protect the legal and financial rights of the government and those affected by government activities (legal and financial rights records) (Source: 36 Code of Federal Regulations [C.F.R.] 1223.2).

Essential Records Packet – An electronic or hard copy compilation of key information, instructions, and supporting documentation needed to access essential records in an emergency (Source: FEMA).

Essential Supporting Activities (ESAs) – Select mission support activities performed by the organization that enable or facilitate the performance of its essential functions (e.g., providing a secure workplace, ensuring computer systems are operating). ESAs are only those activities that would result in severe degradation or failure of an essential function if they were not available (Source: FEMA).

Executive Branch Reconstitution (EBR) Cell – An interagency element composed of personnel from FEMA, the General Services Administration (GSA), the Office of Personnel Management (OPM), and NARA whose mission is to support, assess, and coordinate the reconstitution programs of the executive branch during the resumption of normal operations following a continuity event and inform the National Continuity Coordinator (NCC) of EBR status (Source: FEMA).

Exercise – An event or activity delivered through discussion or action to develop, assess, or validate capabilities to achieve planned objectives (Source: DHS).

External Dependencies – Vital activities and services performed for the organization by partners outside the legal or statutory authority of the organization (Source: FEMA).

Federal – Of or pertaining to the federal government of the United States of America (Source: FEMA).

Federal Continuity Directive – A continuity enterprise document developed and promulgated by the FEMA Administrator, in coordination with the CAG and in consultation with the Interagency Continuity Working Group (ICWG), that directs Federal Executive Branch organizations to carry out identified continuity planning requirements and assessment criteria (Source: FEMA).

Federal Mission Resilience – "The ability of the Federal Executive Branch to continuously maintain the capability and capacity to perform essential functions and services, without time delay, regardless of threats or conditions, and with the understanding that adequate warning of a threat may not be available. Federal Mission Resilience will be realized when preparedness programs, including continuity and enterprise risk management, are fully integrated into the day-to-day operations of the Federal Executive Branch" (Source: 2020 *Federal Mission Resilience Strategy*).

Geographic Dispersion – The distribution of personnel, functions, sites, and other resources in physically different locations from one another (Source: FEMA).

Government Functions – The collective functions of Federal Executive Branch organizations as defined by statute, regulation, presidential directive, or other legal authority (Source: FEMA).

Hardening – Measures taken to mitigate vulnerabilities to the Staff and Organization, Equipment and Systems, Information and Data, and Sites needed to perform an essential function (Source: FEMA).

Hazard – A natural, technological, or human-caused source or cause of harm or difficulty (Source: FEMA).

Headquarters – In this FCD, the term "headquarters" refers to an organization's central head office of operations for either or both essential functions and command and control (Source: FEMA).

High Value Asset (HVA) – "Information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have a serious impact on the organization's ability to perform its mission or conduct business" (Source:

Cybersecurity and Infrastructure Security Agency [CISA], *CISA Insights: Secure High Value Assets [HVAs]*).

Homeland Security Exercise and Evaluation Program (HSEEP) – A program that provides a set of guiding principles for exercise programs as well as a common approach to exercise program management, design, development, conduct, evaluation, and improvement planning (Source: FEMA).

Hot Sites – Sites that operate 24 hours a day with fully operational equipment and the capacity to immediately assume operations upon the loss of the primary site. A hot site requires on-site telecommunications, information, infrastructure, equipment, backup data repositories, and personnel to perform essential functions (Source: FEMA).

Incident – An occurrence, natural or human-caused, that necessitates a response to protect life or property. The word “incident” includes planned events as well as emergencies and/or disasters of all kinds and sizes (Source: FEMA).

Information – Data in a usable form, usually processed, organized, structured, or presented in a meaningful way (Source: DHS).

Interagency Agreement (IAA) – A written agreement between two federal agencies, or major organizational units within an agency, that specifies the goods to be furnished or tasks to be accomplished by one agency (the servicing agency) in support of the other (the requesting agency) (Source: FEMA).

Interagency Board (IAB) – A working group established by the NCC to review and recommend potential PMEFs submitted by organizations before they are submitted to the NCC for final approval (Source: FEMA).

Interagency Continuity Working Group: Issue-specific working groups chartered under the CAG governance structure. ICWGs are designed to bring together subject-matter experts from across the Federal Executive Branch to review, address, and implement requirements outlined in current or emerging national continuity policies (Source: FEMA).

Interoperability – (1) The ability of systems, personnel, or organizations to provide services to and accept services from other systems, personnel, or organizations and to use the services exchanged so that these organizations can operate together effectively; and (2) a condition that is realized among electronic communications operating systems or grids and/or among individual electronic communications devices when those systems and/or devices allow the direct, seamless, and satisfactory exchange of information and services between the users of those systems and devices (Source: FEMA).

Leadership – The senior decision-makers who have been elected (e.g., presidents, governors), designated (e.g., cabinet secretaries, administrators), or appointed (e.g., presidentially appointed or Senate confirmed) to head government organizations, including their components. Depending on the organization, directors and managers may also serve in guiding the organization and making decisions (Source: FEMA).

Legal and Financial Rights Records – "Records needed to protect the legal and financial rights of the Government and of the individuals directly affected by its activities. Much of this information is likely to be CUI" (Source: NARA, *Essential Records Guide*).

Local Government – "(A) a county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; (B) an Indian tribe or authorized tribal organization, or Alaska Native village or organization; and (C) a rural community, unincorporated town or village, or other public entity, for which an application for assistance is made by a State" (Source: 42 U.S.C. § 5122 [8]).

Memorandum of Agreement (MOA) – A document that describes in detail the terms of a relationship or partnership, including the specific responsibilities of and actions to be taken by each of the parties so that their goals may be accomplished (Source: FEMA).

Memorandum of Understanding (MOU) – A document that describes the general area of understanding between parties, explaining the concepts of mutual understanding, goals, and plans shared by the parties (Source: FEMA).

Mission Essential Functions – "Essential functions directly related to accomplishing an organization's mission as set forth in its statutory or executive charter. Generally, MEFs are unique to each organization" (Source: PPD-40, *National Continuity Policy*).

Mission Owner – An individual accountable for performing an essential function that must be sustained during or quickly resumed following a disruption to normal operations. For the Federal Executive Branch, this is the senior accountable government position with the original or delegated authority to lead the Planning, Programming, Budgeting, and Execution (PPBE) and associated risk management of a specific essential function (Source: FEMA).

Mobile Work – Work "characterized by routine and regular travel to conduct work at customer or other worksites as opposed to a single authorized alternative worksite. Examples of mobile work include site audits, site inspections, investigations, property management and work performed while commuting, traveling between worksites or on Temporary Duty (TDY)" (Source: OPM, *Guide to Telework in the Federal Government*).

Multi-Year Strategic Plan (MYSP) – A plan that sets the overall goals and objectives for the continuity program. Organizations should develop a continuity-focused MYSP that provides for the development, maintenance, and review of continuity plans, policies, and procedures to ensure the program remains viable and successful (Source: FEMA).

National Capital Region – Pursuant to the National Capital Planning Act of 1952 (40 U.S.C. § 71), the NCR is the District of Columbia; Montgomery and Prince George's Counties of Maryland; Arlington, Fairfax, Loudoun, and Prince William Counties of Virginia; and all cities now or hereafter existing in Maryland or Virginia within the geographic area bounded by the outer boundaries of the combined area of said counties (Source: FEMA).

National Continuity Coordinator – The Assistant to the President for Homeland Security and Counterterrorism (APHS/CT). The NCC is responsible for coordinating, without exercising directive authority, the integration and execution of continuity policy for Federal Executive Branch organizations (Source: FEMA).

National Continuity Policy – The policy of the United States to maintain a comprehensive and effective continuity capability, composed of continuity of operations and COG programs, to ensure the preservation of our form of government under the Constitution and the continuing performance of NEFs under all conditions (Source: PPD-40, *National Continuity Policy*).

National Essential Functions – "Select functions necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through [continuity of operations], COG and ECG capabilities" (Source: PPD-40, *National Continuity Policy*).

Nongovernmental Organization (NGO) – An entity with an association that is based on the interests of its members, persons, or institutions that has no statutory ties with a government (Source: DHS).

Normal Operations – The broad functions undertaken by an organization that include day-to-day tasks, planning, and execution of tasks. May also be referred to as steady-state operations (Source: FEMA).

Occupant Emergency Plan – A short-term emergency response plan that establishes procedures for evacuating buildings or sheltering in place to safeguard lives and property. Organizations may refer to this plan as the Emergency Plan or Building Closure Plan. Common scenarios that would lead to the activation of these plans include inclement weather, fire, localized power outages, and localized communications outages. These types of events are generally short-lived (Source: FEMA).

Organization Head – The highest-ranking official of an organization, or a successor or designee who has been selected by that official in orders of succession (Source: FEMA).

Out of Area Successor – Designated individuals with decision-making authority who are geographically dispersed from the organization's HQ and other individuals within the order of succession. The Out of Area Successor assumes a leadership position in the event that HQ-based personnel are unavailable (Source: FEMA).

Plan – A proposed or intended method of getting from one set of circumstances to another. A plan is often used to move from the present situation toward accomplishing one or more objectives or goals (Source: FEMA).

Planning, Programming, Budgeting, and Execution – A process to effectively manage strategic planning goals and priorities, engaging in programming analyses to appropriately resource those priorities, defining near-term budget requests in terms of programming decisions, and then executing funding plans and operations and measuring effectiveness (Source: DHS).

Preparedness – Actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from threats and hazards (Source: FEMA).

Primary Mission Essential Functions – "Those MEFs that must be continuously performed to support or implement the uninterrupted performance of NEFs" (Source: PPD-40, *National Continuity Policy*).

Primary Site – The site where an organization's leadership and staff operate on a day-to-day basis (Source: FEMA).

Private Sector – Organizations and individuals that are not part of any governmental structure. The private sector includes for-profit and not-for-profit organizations, formal and informal structures, commerce, and industry (Source: FEMA).

Program – A group of related initiatives managed in a coordinated process to achieve a level of control and benefits that would not be attainable if the initiatives were managed individually. Programs may include elements of related work outside the scope of the program's discrete initiatives (Source: FEMA).

Readiness – The condition of being prepared and capable to act or respond as required (Source: DHS).

Reconstitution – The process by which surviving and/or replacement organizational personnel resume normal operations (Source: FEMA).

Reconstitution Manager – The individual who directs and leads the organization's reconstitution team during all phases of reconstitution, in coordination with the Continuity Program Manager and Mission Owners, making recommendations to leadership on courses of action (COAs) and serving as the primary point of contact between the organization and the EBR Cell (Source: FEMA).

Reconstitution Team – The leadership, staff, and resources dedicated and separate from the organization's identified continuity personnel and responsible for assisting in the establishment of a new normal following a disruption to operations (Source: FEMA).

Recovery – The implementation of prioritized actions required to return an organization's processes and support functions to operational stability following a change in normal operations (Source: FEMA).

Redundancy – The state of having duplicate capabilities, such as systems, equipment, or resources (Source: FEMA).

Relocation – The movement of pre-identified members of an organization's primary operating staff from their primary site to an alternate site to continue performing essential functions when normal operations are disrupted (Source: FEMA).

Remote Work – An arrangement in which an employee, under a written remote work agreement, is scheduled to perform work at an alternative worksite and is not expected to perform work at an agency worksite on a regular and recurring basis. A remote worker's official worksite may be within or outside the local commuting area of an agency worksite (Source: OPM, "Telework Coordinator").

Resilience – The ability to prepare for and adapt to changing conditions and recover rapidly from operational disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents (Source: FEMA).

Response – The capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred (Source: FEMA).

Risk – The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences (Source: FEMA).

Risk Analysis – A systematic examination of the components and characteristics of risk (Source: FEMA).

Risk Assessment – A product or process that collects information and assigns values to risks for the purpose of informing priorities, developing or comparing COAs, and informing decision-making related to an essential function (Source: FEMA).

Risk Management – The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level, considering the associated costs and benefits of any actions taken (Source: FEMA).

Small Agency Council Continuity of Operations Committee – Forum for the review, coordination, and implementation of national continuity policy among Category IV D/As (Source: FEMA).

State – One of the 50 U.S. states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, or the Commonwealth of the Northern Mariana Islands (Source: FEMA).

Steady State – Routine, day-to-day operations (Source: DHS).

Succession – A "formal, sequential assumption of a position's authorities and responsibilities, to the extent not otherwise limited by law, by the holder of another specified position as identified in statute, executive order, or other presidential directive, or by relevant [organizational] policy, order, or regulation if there is no applicable executive order, other presidential directive, or statute in the event of a vacancy in office or a position holder dies, resigns, or is otherwise unable to perform the functions and duties of that pertinent position" (Source: PPD-40, *National Continuity Policy*).

Telework – A flexible work arrangement in which an employee situationally or routinely performs duties and responsibilities from an approved worksite while still reporting to their agency worksite on a regular and recurring basis (Source: FEMA).

Telework Site – An approved worksite where an employee performs his or her duties other than the location from which the employee would otherwise work (Source: FEMA).

Territorial – An unincorporated U.S. insular area, of which there are currently 13: three in the Caribbean (Navassa Island, Puerto Rico, and the U.S. Virgin Islands) and 10 in the Pacific (American Samoa, Baker Island, Guam, Howland Island, Jarvis Island, Johnston Atoll, Kingman Reef, Midway Atoll, the Northern Mariana Islands, and Wake Atoll) (Source: U.S. Department of the Interior, "Definitions of Insular Area Political Organizations").

Test – The demonstration of the correct operation of Staff and Organization, Equipment and Systems, Information and Data, Sites, and processes that support the organization (Source: FEMA).

Threat – Natural or human-caused occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property (Source: FEMA).

Training – Effort to provide organizational staff with the knowledge, skills, and abilities needed to accomplish the key tasks required to perform essential functions (Source: FEMA).

Tribal – Referring to any Indian tribe, band, nation, or other organized group or community, including any Alaskan Native Village as defined in or established pursuant to the Alaska Native Claims Settlement Act (85 Stat. 688 [43 U.S.C. § 1601 et seq.]), that is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians (Source: FEMA).

Warm Sites – Sites that have a minimum acceptable level of infrastructure in place and possess the IT and telecommunications equipment to become operational to support the performance of essential functions as soon as possible, but not later than 12 hours after continuity plan activation. These sites may be in use regularly to support some aspects of normal operations. A warm site typically requires additional personnel, equipment, supplies, software, or customization to be fully operational. Warm sites generally have the resources necessary to sustain critical mission/business processes but lack the capacity to activate all systems or components immediately upon a disruption of normal operations (Source: FEMA).

This page intentionally left blank

Annex G. Acronyms

AAR	After-Action Report
APHS/CT	Assistant to the President for Homeland Security and Counterterrorism
BIA	Business Impact Analysis
BOD	Binding Operational Directive
BPA	Business Process Analysis
CAG	Continuity Advisory Group
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive
C.F.R.	Code of Federal Regulations
CIP	Continuous Improvement Program
CISA	Cybersecurity and Infrastructure Security Agency
COA	Course of Action
COG	Continuity of Government
CSR	Continuity Status Report
CUI	Controlled Unclassified Information
D/A	Department and Agency
DERG	Devolution Emergency Response Group
DHS	Department of Homeland Security
EBR	Executive Branch Reconstitution
ECG	Enduring Constitutional Government
ENS	Emergency Notification System
EOP	Executive Office of the President
ERG	Emergency Response Group
ESA	Essential Supporting Activity

FCAT	Federal Continuity Assessment Tool
FCC	Federal Communications Commission
FCD	Federal Continuity Directive
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act
GETS	Government Emergency Telecommunications Service
GRS	General Records Schedule
GSA	General Services Administration
HF	High Frequency
HQ	Headquarters
HSEEP	Homeland Security Exercise and Evaluation Program
HVA	High Value Asset
IAA	Interagency Agreement
IAB	Interagency Board
ICWG	Interagency Continuity Working Group
INFOSEC	Information Security
IP	Improvement Plan
IT	Information Technology
IT/DR	Information Technology/Disaster Recovery
MEF	Mission Essential Function
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MYSP	Multi-Year Strategic Plan
NARA	National Archives and Records Administration

NCC	National Continuity Coordinator
NCEP	National Continuity Evaluation Program
NCR	National Capital Region
NECP	National Emergency Communications Plan
NEF	National Essential Function
NGO	Nongovernmental Organizations
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NSPM	National Security Presidential Memorandum
NTAS	National Terrorism Advisory System
NTER	National Threat Evaluation and Reporting
OEP	Occupant Emergency Plan
OMB	Office of Management and Budget
ONCP	Office of National Continuity Programs
OPM	Office of Personnel Management
OPSEC	Operations Security
OSTP	Office of Science and Technology Policy
PACE	Primary, Alternate, Contingency, Emergency
PIN	Personal Identification Number
PMEF	Primary Mission Essential Function
PPBE	Planning, Programming, Budgeting and Execution
PPD	Presidential Policy Directive
QL	Quick Look
RSR	Reconstitution Status Report

SF	Standard Form
SLTT	State, Local, Tribal, and Territorial
TDY	Temporary Duty
TSP	Telecommunications Service Priority
U.S.C.	United States Code
USPS	United States Postal Service
VRA	Vacancies Reform Act
WMD	Weapon of Mass Destruction
WPS	Wireless Priority Service