



Continuity Guidance Circular

February 2018 (2024 update)

FEMA Office of National Continuity Programs



FEMA



A key underpinning of a ready nation is addressing the unmitigated threats and hazards to the United States government that present real risks to the whole community. The collective work across our nation to counter these risks is vital to assuring the performance of the Nation's most critical functions at all levels. This updated Continuity Guidance Circular (CGC) builds on the foundation of existing policy and doctrine while representing an adaptive pivot to address current and nascent risks to the Nation.

The threat landscape is ever-evolving, and threats presented by nation-states and climate-based concerns remain at the forefront. Cyber threats and the increased consequences we face from natural disasters reinforce the criticality of our mitigation work. In accordance with the Federal Emergency Management Agency's role in providing planning guidance to our whole community partners, I am pleased to issue the CGC to help all organizations manage risks to their essential functions. This updated CGC reflects a pivot in national continuity policy and doctrine, intending to engage more directly with those leading and executing our nation's most essential functions while supporting them in mitigating potential impacts to their missions. Additionally, this CGC includes a new Continuity Planning Framework, providing a structure for the development, evaluation, sustainment, and enhancement of essential functions and risk management services, including a whole of government and whole of community perspective.

A collaborative approach to holistic risk management is essential to realizing national continuity of government outcomes and strengthening overall U.S. readiness to threats and hazards we face today and in the future. With this guidance and the renewed emphasis on Mission Owner leadership and the establishment of the new Planning Framework, we continue our adaptive and agile mitigation of impacts to the Nation and our interests.

Deanne Criswell

Administrator
Federal Emergency Management Agency

Continuity Guidance Circular Table of Contents

Overview Continuity Guidance Circular (CGC)	1
CGC Vision	1
CGC Purpose	1
CGC Objectives	2
CGC Scope	2
Chapter 1 Getting Started	3
Guidance Principles	3
Guidance and Standards	3
Whole Community Integration	4
Chapter 2 Initiating Planning	8
Continuity Planning Framework	8
Setting Up a Program	9
Roles and Responsibilities	10
Leadership Support and Mission Owner Engagement	11
Continuity Concept of Operations	12
Chapter 3 Building a Capability	16
Step 1: Identify Essential Functions	16
Step 2: Identify Requirements	20
Step 3: Conduct a Risk Assessment	21
Risk Mitigation Approaches	22
Step 4: Identify and Implement Continuity Options	24
Chapter 4 Maintaining a Capability	34
Technical Assistance and Training	34
Evaluation	34
Continuous Improvement Planning	35
Updating and Reviewing Plans and Programs	35
Resource Direction and Investment	36
Multiyear Strategic Planning	37
Conclusion	38
Annex A Continuity Program Guidance	39
Annex B Authorities and References	41
Annex C Definitions	42
Annex D Acronyms	46



Overview: Continuity Guidance Circular (CGC)

CGC Vision

The vision for continuity is a more resilient nation through whole community integration of continuity plans and programs to sustain essential functions under all conditions. To achieve this vision, this Continuity Guidance Circular is flexible and adaptable for a broad range of audiences, threats, and capabilities in order to meet the needs of any given organization and can evolve to suit the changing environment.

THE Vision

The vision for continuity is a more resilient nation through whole community integration of continuity plans and programs to sustain essential functions under all conditions.

CGC Purpose

This Continuity Guidance Circular serves as a resource for non-governmental organizations (NGOs), private-sector entities, state, local, tribal, and territorial (SLTT) governments, schools, academic institutions, and federal entities. This CGC aims to build continuity capabilities, assuring the performance of essential functions and critical services communities across the Nation. This includes (1) providing an understanding of continuity options; (2) offering guidance on how to integrate these options into operations; and (3) supporting the development of tools and resources. This circular does not make current continuity plans and programs obsolete. However, to promote consistency across the Nation, entities are encouraged to review this CGC and update plans and capabilities as necessary. This assists in enhancing jurisdictional continuity plans and capabilities and aligning those plans and capabilities with national continuity doctrine, as identified in this circular. This circular supersedes the previous *Continuity Guidance Circular*, dated February 2018.

Why Continuity?

Day to day, the whole community works together to provide essential functions, capabilities, and services to each other.

An event can disrupt the performance of essential functions, capabilities, and services at all levels.





CGC Objectives

The objectives of this circular are to:

- Describe activities that support establishing and maintaining a comprehensive and effective continuity program to ensure the resilience of essential functions at all levels, under all conditions, and ultimately the preservation of our form of government under the Constitution.
- Provide a comprehensive perspective to foster the integration of continuity capabilities into operations.
- Outline continuity guidance principles to inform planning, coordination, and operations.
- Define scalable, flexible, and adaptable continuity options, as well as key roles and responsibilities for building and integrating continuity plans across the whole community.

CGC Scope

Planning across the full range of continuity operations is an inherent responsibility of every level of government and across the whole community. This circular fosters unity of effort for continuity of operations, continuity of government at all levels, and enduring constitutional government planning by providing common doctrine and purpose.

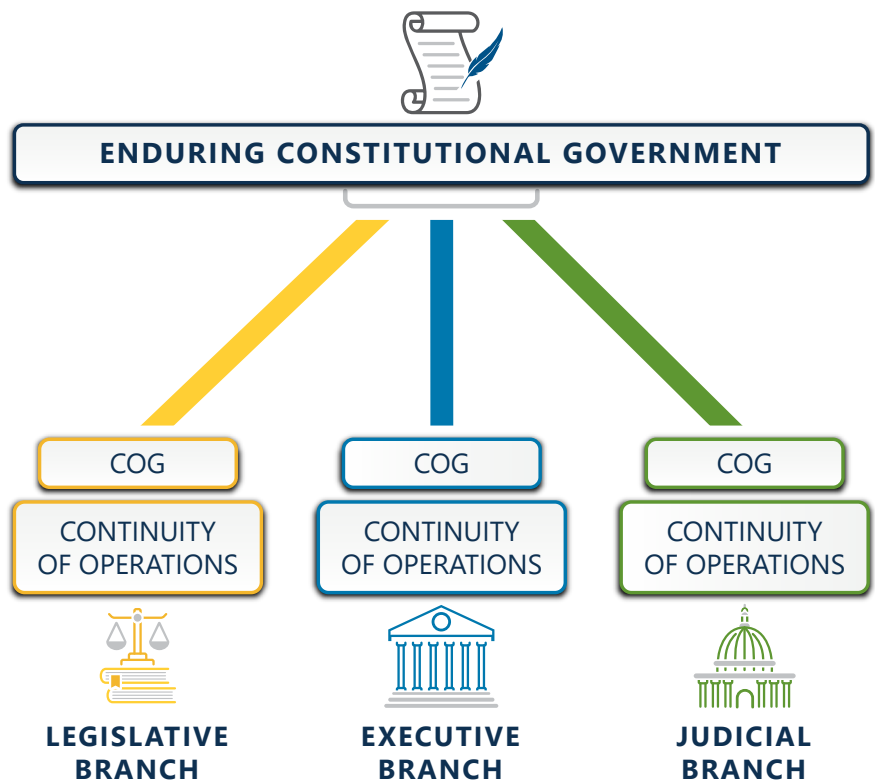
Continuity of operations is the ability of an organization to continue essential functions, provide essential services, and deliver core capabilities during a disruption to normal operations. Effective continuity of operations can be attained only through the integration and unified efforts of an organization’s leadership, who are accountable for the performance of essential functions and the continuity program at all levels.

Continuity of government (COG) is an outcome of a viable continuity capability for a branch of government. COG requires a coordinated effort within the executive, legislative, and judicial branches to ensure essential functions during a disruption to normal operations. COG is intended to preserve the statutory and constitutional authority of elected officials at all levels of

government across the United States. Achieving COG requires an enhanced level of resilience, coordination, communication, and deconfliction among the organizations and positions most critical to the continued functioning of the government.

Additional information about COG may be found in FEMA’s *Guide to Continuity of Government for State, Local, Tribal, and Territorial Governments*.¹

Enduring constitutional government (ECG) is the cooperative effort among the executive, legislative, and judicial branches to preserve the constitutional framework under which people are governed. ECG focuses on the ability of all three branches of government to execute constitutional responsibilities, provide for orderly succession and an appropriate transition of leadership, and support essential functions during an emergency. Jurisdictions might not delineate separate planning efforts for COG and ECG, especially among smaller communities; however, the goal of ensuring a functioning government remains the same.



¹ Guide to Continuity of Government for State, Local, Territorial, and Tribal Governments (fema.gov)



Chapter 1: Getting Started

Before beginning to develop or update continuity plans and procedures, an organization should create an overall strategy to build resilience into operations that has buy-in from elected officials or organizational leadership. This section identifies foundational elements of a continuity capability that will increase the success of continuity planning and operations. Staff responsible for continuity should consider, implement, and enhance these elements to ensure the success of their organization.

Guiding Principles

The potential for no-notice emergencies—including localized natural hazards, accidents, technological emergencies, and terrorist attacks—requires strong continuity plans that enable communities and organizations to continue their essential functions. This planning is guided by three primary principles: **(1) Preparedness and Resilience**; **(2) Whole Community Engagement**; and **(3) Scalable, Flexible, and Adaptable Continuity Capabilities**.

1. Preparedness and Resilience

A prepared and resilient nation is built on the foundation of prepared and resilient individuals, communities, and the organizations that comprise it. Continuity is an important element of preparedness and an integral part of each core capability across the five mission areas in the National Preparedness System: protection, prevention, mitigation, response, and recovery. The National Preparedness Goal identifies core capabilities, which are activities that address the greatest risks to the Nation. A comprehensive continuity program increases the likelihood that organizations can perform essential functions and deliver core capabilities and essential services.

The National Preparedness System and the National Incident Management System (NIMS), with the foundational support of continuity, enables the Nation to be able to prevent, protect against, respond to, and recover from any incident with minimal disruptions to the functions, and services that citizens expect.

2. Whole Community Engagement

The Nation is stronger when the communities that comprise it are resilient to threats and hazards. Per the National Preparedness Goal, “whole community” is defined as a “focus on enabling the participation in national preparedness activities of a wider range of players from the private and nonprofit sectors, including NGOs and the general public, in conjunction with the participation of all levels of government in order to foster better coordination and working relationships.” Every community and organization, no matter how large or small, has essential functions that support the continuation and resilience of the Nation. No single entity, not even the federal government, can perform all the functions and services without the support of the rest of the Nation. Multidisciplinary and multijurisdictional partnerships are critical in developing and sustaining an effective continuity capability.



3. Scalable, Flexible, and Adaptable Continuity Capabilities

A comprehensive continuity program and culture require continuity programs and capabilities to be scalable, flexible, and adaptable to meet evolving requirements. As needs grow and change, continuity capabilities must remain nimble and adjustable to achieve the vision set forth in this document.

Guidance and Standards

Numerous public and private-sector standards, laws, codes, and guidelines exist to guide continuity planning and operations and



their integration with preparedness, emergency management, mitigation, and recovery. Under Presidential Policy Directive 40 (PPD-40), *National Continuity Policy*, FEMA must develop and promulgate continuity programs and planning requirements for Federal Executive Branch organizations and develop and promulgate continuity planning guidance for SLTT governments, NGOs, and private-sector critical infrastructure owners and operators. Federal Executive Branch organizations are governed by the requirements outlined in PPD-40 and the Federal Continuity Directives (FCDs). Many states have gubernatorial mandates requiring state agencies to develop continuity plans. Numerous counties, municipalities, and other government organizations require continuity programs. The public and private sectors, such as healthcare and banking, have accreditation and regulatory requirements that encompass business continuity principles.

Organizations should first identify existing applicable continuity regulations or requirements. In the absence of mandated requirements, an organization should identify the continuity guidance and principles most applicable to its organization. This circular outlines a continuity planning framework with principles and tools that organizations can adopt. Deciding which continuity options (i.e., the actions or activities that enable the continuation of essential functions and requirements) to use depends on many considerations, including resources, the size of the organization, and organizational functions. Ultimately, implementing and adhering to a standardized continuity principle or set of principles will further enhance the preparedness of an organization, its community, and the Nation.

Municipal and state governments without a mandate for continuity planning should consider developing a comprehensive policy to guide the planning and preparedness of those organizations on which the community depends. Establishing or adopting a standard enables a coordinated planning process across different organizations and a policy-level framework to guide decisions made during continuity planning and implementation.

Whole Community Integration

An all-inclusive approach focuses efforts and enables a full range of stakeholders to participate in continuity activities and maintain resilient communities. Government resources alone cannot meet all the needs of those affected by disasters or other disruptive incidents.



All elements of the community must be engaged and integrated in order to continue essential functions during any disruption to operations.

The most effective partnerships within a community capitalize on multidisciplinary coalitions and all available resources, including identifying, developing, fostering, and strengthening new and existing coordinating structures to create a unity of effort and expand the capacity of all those involved. Many community organizations and partners have active roles in several sectors and priorities simultaneously. Proactive efforts to collaborate and coordinate before and during incidents reduce disruptions to essential functions and critical services.

FEMA's Comprehensive Preparedness Guide (CPG) 101, *Developing and Maintaining Emergency Operations Plans*,² outlines the importance of engaging in community-based planning (i.e., planning for the whole community). Continuity-specific roles of whole community members include the following:

- **Individuals, Families, and Households**

Individuals, families, and households play an important role in executing essential functions and providing critical services, so impacts to people may jeopardize the continued performance of essential functions.

² Developing and Maintaining Emergency Operations Plans, Comprehensive Preparedness Guide (fema.gov)



- **Communities**

Engagement of community groups in promoting a culture of continuity through identifying and capitalizing on shared needs and capabilities serves as a force multiplier to ensure the delivery of essential services and functions during an incident.

- **NGOs**

NGOs are key partners in continuity planning and activities through their role in delivering important and varied services and bolstering government efforts at all levels. Not only should NGOs have their own continuity programs to ensure the continued performance of essential functions, but they should be integrated into continuity planning efforts at all levels of government.

- **Private-Sector Entities and Critical Infrastructure Sectors**

Some businesses play an essential role in protecting critical infrastructure systems and implementing plans to rapidly reestablish normal commercial activities and critical infrastructure operations following a disruption. Collaborating with the private sector, where most critical infrastructure resides, is crucial to ensuring the continuity of essential functions and critical services. The private sector also plays a key role in reconstituting organizations and governments. These organizations are vital to the Nation's ability to continue to perform essential functions and provide critical services.

- **Local Governments**

Local governments provide critical services, including the protection of the health, safety, and welfare of their residents and visitors. Local government continuity plans are often closely tied to emergency operations plans and community preparedness systems. Due to the essential nature of local government functions, continuity planning and operations are

a core component of government administration. State, tribal, and territorial governments and the federal government rely on local governments to have effective continuity programs. The essential functions of all levels of government contribute directly to national resilience through assured COG and ECG.

- **State and Territorial Governments**

State and territorial governments serve an integral role as a conduit for continuity coordination, planning, and operations among federal agencies and local governments. All levels of government must be able to coordinate and work together to ensure the integration of continuity planning and operational efforts.

- **Tribal Governments**

As sovereign nations, tribal governments govern and manage the safety and security of their lands, residents, and those who live and work on tribal lands. Along with other partners, stakeholders, and all levels of government, tribal governments play a vital role in national resilience.

- **Federal Government**

It is the policy of the United States to maintain a comprehensive and effective continuity capability by ensuring a coordinated effort within and among the executive, legislative, and judicial branches of the government to perform essential functions across a full spectrum of threats and hazards. Because of the interdependent nature of essential functions, federal government organizations cannot sustain and perform them without the support and integration of efforts by federal and non-federal entities. Most federal organizations have regional or field offices that may participate with state and local governments in continuity planning through working groups, integrated training, and evaluation events. It is important to make the most of any available opportunities to further integrate and collaborate with federal partners.

- **Federal Emergency Management Agency**

Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities*, directs FEMA to “assist in the implementation of national security emergency preparedness policy by coordinating with the other federal departments and agencies and with state and local governments.” PPD-40, *National Continuity Policy*, designates FEMA to, among other tasks, “develop and promulgate continuity planning guidance to state, local, territorial, and tribal governments, NGOs, and private-sector critical infrastructure owners and operators; make continuity planning and exercise funding available, in the form of grants as provided by law, to state, local, territorial, and tribal governments; make available, as requested, continuity planning and exercise technical assistance to private-sector critical





infrastructure owners and operators; to support and facilitate regional and state-level continuity working groups; and, at a minimum, conduct annual continuity events to address federal and non-federal government continuity planning and other elements of a viable continuity program.”

Integration of Resources and Plans

The continuity of essential functions and the provision of critical services cannot be an afterthought for organizations. Continuity is more than just a good business practice that needs to be incorporated into day-to-day planning; it helps communities work together to reduce vulnerabilities and recover from an incident.

An integrated and inclusive approach to emergency management is based on solid general management principles and the common theme of protecting life and property. Emergencies are not isolated, and continuity planning does not exist in a vacuum. Planners must coordinate continuity plans and programs with incident management, occupant emergency plans, and emergency operations plans (EOPs). Proper training and evaluation among the whole community helps delineate roles and responsibilities and deconflict procedural, resource, and personnel issues.



National Incident Management System and Incident Command System

Organizations should integrate continuity planning with incident management planning and operations, including the responsibilities outlined in the National Planning Frameworks.³

Continuity does not delineate new procedures for incident management activities other than already established protocols; however, organizations with incident management responsibilities must incorporate requirements to perform these functions into continuity planning. Integration is especially key for interagency coordination groups that monitor or convene during an incident. The lead agency for these interagency groups should develop and share continuity plans to ensure the group’s continued capability regardless of circumstance.



Occupant Emergency Plans and Facility Emergency Plans

Occupant emergency programs, occupant emergency plans, and facility emergency plans establish basic procedures for safeguarding lives and property in and around a facility during emergencies. These plans are intended to minimize the risk to personnel, property, and other assets. However, the plans need to be

coordinated to ensure a seamless transition from an emergency, as facility inaccessibility or staff unavailability can lead to a continuity plan activation. In certain emergencies, evacuation of a facility or deployment of staff may place individuals’ safety and health in danger. Continuity Planners should account for such situations and plan accordingly to ensure that essential functions and critical services outlined in these plans are continued safely.



Emergency Operations Plans (EOPs)

EOPs describe who will do what, when, with what resources, and by what authority before, during, and immediately after an emergency. A jurisdiction’s EOP is the centerpiece of its comprehensive emergency management

efforts. Continuity planning enables the successful implementation of an EOP during and after an emergency by ensuring that essential functions, critical services, and visible leadership are readily available. FEMA’s CPG 101 is designed to help both novice and experienced planners navigate the EOP planning process. The guide provides information and instruction on the fundamentals of planning and its application.



Information Technology and Disaster Recovery Plans (IT/DR)

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. An IT/DR plan does not account for how an organization will continue its essential functions during an emergency. It does, however, impact an organization’s continuity plan and operations by identifying recovery time objectives for key systems that support the performance of functions, including essential functions.



Hazard-Specific Response Plans

Some organizations may have hazard-specific response plans. For example, a pandemic or infectious disease plan is a strategy for organizations to mitigate the illness, suffering, and death of their staff while sustaining their

ability to provide services and perform essential functions during a period of significant employee absenteeism. Aspects of an organization’s pandemic or infectious disease plan may be used in non-pandemic incidents that may impact personnel’s ability to report to work. Because a pandemic or other hazard-specific response may trigger a continuity plan activation, such plans have an important role in an organization’s overall continuity plan and should be coordinated.

³ National Planning Frameworks | FEMA.gov



Business Continuity Plans

Business continuity plans outline the processes that enable an organization to continue its essential functions following a disruption to normal operations. Business continuity plans focus on key variables that recover the delivery

of products and services that allow businesses to minimize lost revenues and return to normal operations. Businesses often have a direct role in ensuring the resilience of the communities in which they reside.

(Note | The information in this circular does not supersede other business continuity guidance and direction but is meant to supplement and provide context for a holistic view of whole community resilience through the execution of robust and integrated continuity plans.)

*FEMA has developed a supporting **Continuity Resource Toolkit** that provides examples, tools, and templates for implementing this circular. In the future, FEMA will continue to build and distribute tools and information to assist federal and non-federal entities in developing and maintaining a successful continuity program and plan.*

*The Toolkit is available at **Continuity Resource Toolkit | FEMA.gov.***





Chapter 2: Initiating Planning

Planning across the full range of continuity operations is an inherent responsibility of all levels of government and the whole community. The alignment of resources with continuity plans and procedures can ensure essential functions continue during a disruption.

Continuity Planning Framework

The Continuity Planning Framework updates and builds upon existing national continuity policy and serves as the foundation for a mission-focused, operational approach to mitigate impacts from threats and hazards. Additionally, it requires leadership to integrate continuity into day-to-day operations.

analyses to identify which operations, tasks, or functions cannot be interrupted and which may be reduced, deferred, or postponed. Organizations should prioritize potentially limited resources by understanding the requirements of each planning factor—Staff & Organization, Equipment & Systems, Information & Data, and Sites—to accomplish their mission. By considering the vulnerabilities of each planning factor to the full spectrum of threats and hazards, organizations will better understand the overall risk to each essential function.

National Continuity Planning Framework Planning Factors:

- Staff & Organization
- Information & Data
- Equipment & Systems
- Sites

The Framework reinforces organizations' all-hazards approach to continuity planning to manage the consequences of any disruption to normal operations, up to and including those that occur with little to no warning.⁴

In the event of a disruption to normal operations, organizations will likely face limitations on their resources, assets, and capabilities. In this constrained environment, functions with little or no allowable downtime should be prioritized. Organizations should conduct

Figure 1 illustrates the overall process for achieving essential function resilience. Organizations should identify their essential functions, determine the planning factors needed to accomplish those functions, conduct risk assessments for each planning factor, and identify and implement continuity options addressing the areas of greatest vulnerability.

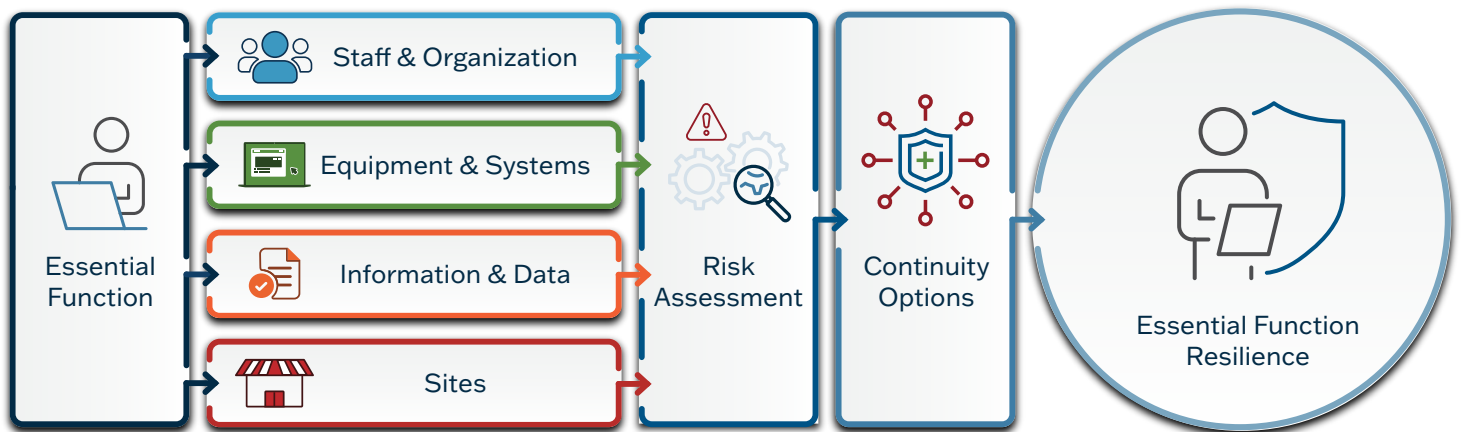


FIGURE 1 | Continuity Planning Framework

⁴ Federal Continuity Directive: Continuity Planning Framework for the Federal Executive Branch (fema.gov)



Essential functions are a subset of organizational functions that are determined to be critical activities. These essential functions are then used to identify supporting tasks and resources that must be included in the organization’s continuity planning process.

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

The Continuity Planning Framework can be applied across continuity of operations, COG, and ECG planning at all levels by providing a logic model to understand resource needs, vulnerabilities, and risks.

Setting Up a Program

Organizations should create and maintain a viable continuity program to responsibly ensure their essential functions continue. Through a standardized program management structure for their continuity programs, organizations can guide leaders, allocate resources, and create an environment in which staff can make informed decisions to improve resilience. When initiating continuity planning, organizations are encouraged to:

- **Become knowledgeable about the current program.** Read existing plans and procedures. If a continuity plan or procedures do not exist, planners should determine if there are any other emergency plans that interface with continuity, such as EOPs, pandemic plans, and cybersecurity plans.
- **Identify continuity program planning roles and responsibilities.** Organizations should title and fill roles within the continuity program and planning effort to clearly articulate roles and responsibilities. Depending on size, mission, and resources, organizations and jurisdictions may choose to combine responsibilities under one or more of these roles.

To assist organizations with developing and maintaining continuity plans and programs, FEMA has established a continuity training

program that addresses the full spectrum of continuity planning. The Continuity Excellence Series certificate program enhances the skills and expertise of continuity practitioners at all levels. For additional details, please visit the [Continuity Resource Toolkit | FEMA.gov](#).

- **Establish a continuity planning team.** One person alone cannot develop the continuity plan. Once a continuity plan is developed, this team can continue to meet periodically to update the plan and develop training and exercises. The continuity planning team should consist of representatives from:
 - **Essential Functions and Services Offices**
These offices perform the daily essential functions and services and are responsible for their risk management and continuation of operations through disruptions. Their expertise and knowledge are needed to inform a wide range of continuity planning efforts.
 - **Information technology (IT)**
Technology includes communications, critical systems, and data. It is the foundation of many tasks, activities, functions, and capabilities in an organization. Experts in these areas play a key role in ensuring required resources are available in a continuity activation.
 - **Human Resources**
Organizations should coordinate with human resources representatives when developing continuity plans and programs. Topics to address include incorporating commonly requested reasonable accommodations into the plan, designating employees as continuity personnel, developing telework protocols to support continuity operations, and establishing accountability procedures and timekeeping during disruptions to normal operations.
 - **Facilities Management**
Facility managers can assist with ensuring a ready and available alternate site, if chosen as a mitigation strategy. In addition, they maintain responsibility for assessing damage to the primary operating site and planning for reconstitution.





- **Comptroller**

Organizations should align and allocate the resources needed to implement their continuity option(s). Through the budgeting and planning process, an organization's leaders and staff ensure the availability of critical continuity resources needed to continue the performance of the organization's essential functions before, during, and after a disruption to normal operations.

- **Security**

Security strategies are needed to protect plans, personnel, sites, and capabilities and to prevent adversaries from disrupting continuity operations.

- **Legal**

An organization's legal department or equivalent should review the delegations of authority, orders of succession, and memoranda of agreement/understanding (MOAs/MOUs) to ensure legal sufficiency. Legal departments or the equivalent may also interpret laws informing timelines associated with restoring essential functions.

- **Bargaining unit or union representation, if applicable**

Organizations should work with bargaining units and labor unions to develop and negotiate procedures that may impact bargaining unit employees.

- **Develop a project plan, timelines, and milestones.**

Identifying a project plan, timelines, and milestones will assist the team in facilitating an efficient and effective planning effort.

- **Identify preliminary budgeting and resource requirements.**

An organization should develop a detailed budget during the continuity planning process once essential functions, mitigation strategies, and resource requirements are identified. However, the team should also identify an initial budget estimate, particularly for the expected costs and resources needed to develop the continuity capability.

- **Leadership and Elected Officials**

The requirements and responsibilities of leadership and elected officials are discussed in more detail in the next section. Leadership and elected officials include the Continuity Coordinator and Mission Owners and are ultimately responsible for ensuring their organizations can continue to perform essential functions.

- **Mission Owners**

The Mission Owner is the senior accountable position with the original or delegated authority to lead the planning, budgeting, accomplishment, and associated risk management of a specific essential function.

- **Continuity Coordinator**

The Continuity Coordinator is the senior accountable official, designated by leadership or elected officials, who is responsible for oversight of the organization's continuity program and represents their organization externally in coordinating continuity efforts. Continuity Coordinators are supported by a Continuity Program Manager and other Continuity Planners within subcomponent levels throughout the organization or government.

- **Continuity Program Manager**

A senior Continuity Planner should be responsible for coordinating overall continuity activities. This individual is designated by and reports to the Continuity Coordinator, manages day-to-day continuity programs, coordinates the continuity plan, and may represent the organization's program externally, as appropriate.

- **Continuity Planner**

The Continuity Planner is responsible for developing and maintaining an organization or subcomponent continuity plan and integrating and coordinating the continuity plan with broader organizational or governmental guidance, requirements, and initiatives.

- **Continuity Planning Team**

The continuity planning team is comprised of representatives from offices across the spectrum of the organization to inform and assist the continuity planning and program efforts.

- **Continuity personnel**

During a disruption to normal operations, organizations may mobilize specific, pre-identified personnel to sustain essential functions. These personnel may be known by various organizational terms to indicate their critical nature in the continuation of essential functions.

Roles and Responsibilities

People are the most valuable resource in any organization. The structure of leadership—including Mission Owners, management, and staff (both government employees and contractor personnel)—should be organized to support decision-making and the performance of essential functions. During a disruption to normal operations, organizations may mobilize specific, pre-identified personnel as necessary to sustain essential functions. These include those personnel who provide organizational leadership with the advice, recommendations, and functional support needed for the continued performance of essential functions.



- **All Employees**

Because a continuity plan activation impacts the entire organization, all employees are responsible for understanding their roles and responsibilities under the continuity plan.

Leadership Support and Mission Owner Engagement

Because of the role that continuity plays in our Nation's resilience, its importance must be recognized by elected officials, organizational leadership, and Mission Owners. Elected officials and organizational leadership should articulate a commitment to continuity for a culture of continuity and preparedness to permeate throughout the organization. Mission Owners are ultimately responsible for the resilience of their operations but require guidance and support from higher-level and peer leaders. Coordination among leadership, including elected officials and Mission Owners, is necessary to oversee a comprehensive planning environment by integrating continuity into day-to-day operations, empowering personnel, and developing relationships with internal and external stakeholders to build a resilient community and Nation. Leadership, Mission Owners, Continuity Coordinators, and Continuity Program Managers working together in the continuity planning process increases the likelihood that investments are made in continuity capabilities and that plans are used when needed.

Leadership engagement in continuity assurance should be integrated with the various programs, including assessments and grants across the jurisdiction, to ready it for impacts. FEMA's CPG 201, *Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide*,⁵ offers information for communities to collect specific, quantitative information while providing context so that they can have more detailed and actionable data on their capabilities and identify capability gaps. Organizations may use this information to address and prioritize areas for improvement based on the capability solution areas of planning, organization, equipment, training, and exercises (POETE). Several options and tools are available to assist organizations in obtaining the support of leadership and elected officials for the continuity program.

- **Identify preparedness or emergency management forums or working groups** in which your leadership can participate. When leadership is exposed to the initiatives and plans in which other organizations and leaders are engaging, they may be encouraged to provide similar support to your organization. Forums also allow for highlighting best practices, lessons



learned, and interdependencies between your organization and others.

- **Conduct technical assistance and training.** It is important for organizations to ensure that all levels of leadership and Mission Owners are familiar with their roles and responsibilities during a disruption to normal operations, especially if they differ from the steady-state environment. Leadership and Mission Owners should be engaged through technical assistance and training activities to develop an understanding of the orders of succession, delegations of authority, and required decision-making associated with continuity options.
- **Conduct evaluation events.** The evaluation of continuity capabilities is essential to demonstrating, assessing, and improving an organization's ability to execute its essential functions when normal operations are disrupted.
- **Relate continuity to your organization's mission and priorities.** Leadership is focused on and understands the mission and priorities of its organization. Communicating the benefits and value of continuity by articulating linkages to them can enhance leadership support for the continuity program.
- **Include continuity as a critical element of leaders' evaluations and performance plans.** Leadership and elected officials are ultimately responsible for whether an organization or government can continue essential functions and services under all circumstances. Including continuity planning milestones and metrics within a leader's performance plan or evaluations helps ensure a continual focus and commitment to the continuity program.

⁵ Comprehensive Preparedness Guide (CPG) 201, 3rd Edition (fema.gov)



Continuity Concept of Operations

A comprehensive and integrated continuity program and plan will enable a more rapid and effective response to and recovery from all emergencies. While an organization needs the four planning factors to perform its essential functions, it also needs to be able to execute plans that spell out what to do with those necessary resources. By continuing the performance of essential functions during and after a disruption to normal operations, the whole community supports the performance of the National Essential Functions (NEFs), maintains COG and ECG, and ensures that critical services are provided to the Nation.

Phases of Continuity

Implementation of a continuity plan is intended to continue or rapidly resume essential functions following a change to normal operating conditions. There are four phases of continuity: **Readiness and Preparedness, Activation, Continuity Operations,** and **Establishing a New Normal.** These four phases should be used to build continuity processes and procedures, establish goals and objectives, and support the performance of organizational essential functions during a disruption to normal operations.

Phase I: Readiness & Preparedness

Readiness is the ability of an organization to respond to a continuity activation. 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. Although readiness is a function of planning and training, it is ultimately the responsibility of an organization's leadership to ensure that an organization can perform its essential functions before, during, and

after all-hazards emergencies or disasters.

This phase includes all organizational continuity readiness and preparedness activities:

- The development, review, and revision of plans.
- Provision of guidance to all staff.
- Technical assistance and training activities.
- Evaluation activities, such as testing and exercising.
- Risk management, including identifying mitigation strategies.
- Conducting corrective action planning and continuous improvement activities.
- Incorporation of readiness postures and preparedness measures into daily activities.

Phase II: Activation

This phase includes the assessment of potential or actual event impacts and the activation of continuity plans and procedures to enable the continued performance of essential functions. It also includes the activation of personnel, essential records and databases, and equipment involved with these functions. Continuity plan and procedures activation and execution will require the use of one or more continuity options, depending on the incident and its effect on normal operations.

Organizations should outline the process for activating the continuity plan and identify who has authority to activate it (see Roles and Responsibilities on page 10). An organization may convene a team of senior leadership and/or staff to review the situation and determine if the continuity plan should be activated.

Organizations should identify triggers to assist leadership in deciding to activate continuity plans. Triggers assist personnel in recognizing

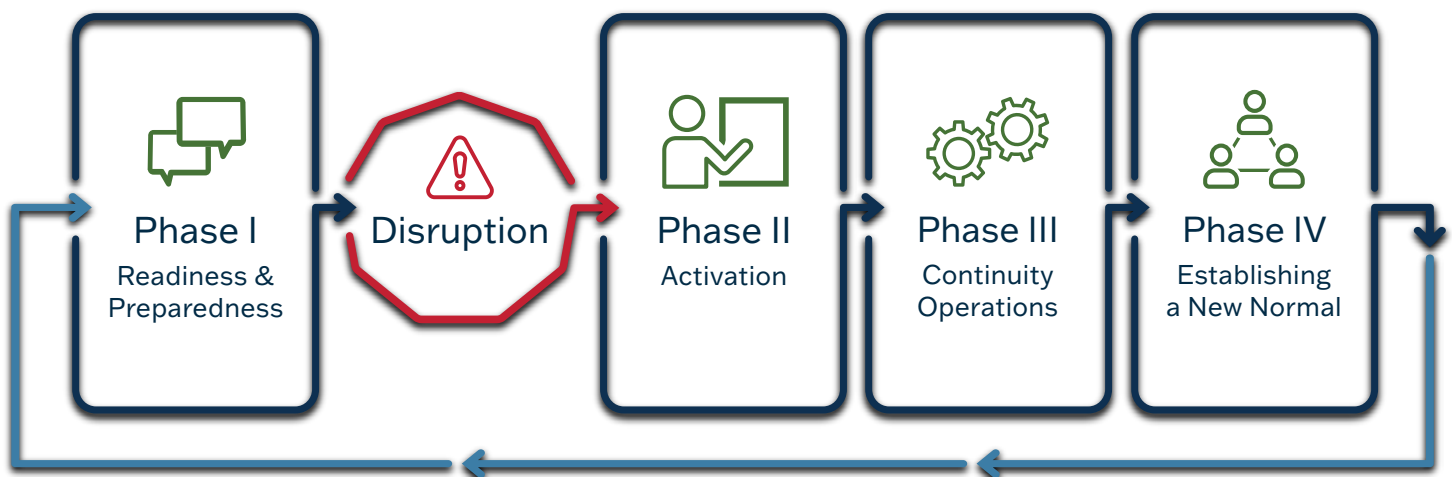


FIGURE 2 | The Four Phases of Continuity



when continuity plan activation is required and enable a smoother transition to continuity operations. Examples of scenarios that may require the activation of continuity plans include the following:

- An organization receives notification of a credible threat, which leads it to enhance its readiness posture and prepare to take the necessary actions.
- An organization experiences a disruption to one or more elements of the essential functions and services planning factor elements (Staff & Organization, Equipment & Systems, Information & Data, and Sites).
- Evacuation orders for the immediate or geographically affected area.

Identifying active and passive activation triggers assists leadership, Mission Owners, and continuity personnel in recognizing when continuity plan activation is required and enables a smoother transition to continuity operations.

The activation phase includes the following activities:

- Gaining situational awareness and assessing event impact on essential function(s).
- Deciding to activate the continuity plan when normal operations are fully or partially disrupted.
- Alerting personnel, including devolution and mutual aid partners, alternate sites, subordinate and headquarters organizations, all employees, and other stakeholders.
- Implementing continuity options, such as relocating to alternate sites, devolving, activating mutual aid agreements, transitioning to alternate systems, and/or testing.

An organization must also consider how it transitions from day-to-day operations to continuity operations. Can functions be interrupted long enough for personnel to establish operations somewhere that is unaffected by the disruption? If not, would a partial devolution or mutual aid agreement assist the organization in sustaining essential functions? Or can personnel perform essential functions from a telework location? Each organization is different, and there are a variety of options to ensure that essential functions and critical services are not interrupted.

Phase III: Continuity Operations

This is the phase where organizations implement and execute the options identified in the continuity plan to ensure that the essential functions are accomplished. The continuity operations phase includes, but is not limited to, the following:

Active triggers initiate actions because of a deliberate decision by jurisdictional 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.

- Accounting for personnel, including their positions' successors, as appropriate.
- Employing continuity options in the performance of essential functions and services.
- Establishing communications with interdependent organizations and other internal and external stakeholders, including the media and the public.
- Preparing for the reconstitution of the organization's operating site and establishing a new normal.
- Providing guidance to all personnel.
- Preparing for the recovery of the organization.

Phase IV: Establishing a New Normal

During the final phase of continuity, organizations transition from the alternate site(s) to either the normal primary site, another temporary site, or a new permanent site, as well as focus on confirming the success of the organization's reconstitution operations and establishing a new normal. This phase includes, but is not limited to, the following:

- Establishing that the organization is fully capable of accomplishing all organizational functions and operations using new or restored Staff & Organization, Equipment & Systems, Information & Data, and Sites.
- Returning activated continuity staff to their normal duty assignments.
- 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 After-Action Report (AAR) and incorporating approved recommendations into a continuous improvement program (CIP).
- Revising and updating plans, procedures, and checklists as appropriate as part of the Readiness & Preparedness Phase.



TABLE 1 | Phases of Continuity | Key Tasks

 PHASE I Readiness & Preparedness	 PHASE II Activation	 PHASE III Continuity Operations	 PHASE IV Establishing a New Normal
<ul style="list-style-type: none"> • Developing, reviewing, and revising plans. • Incorporating readiness postures and preparedness measures into daily activities. • Preparing personnel, including the provision of guidance to all staff, internal and external coordination, and information sharing. • Conducting evaluation activities, including the identification of risks. • Mitigating risks through corrective actions execution. 	<ul style="list-style-type: none"> • Assessing potential or realized event impacts. • Activating continuity plans fully or partially. • Moving personnel. • Distributing notifications and internal and external messaging. • Testing contingency capabilities. • Submitting any required status reports. 	<ul style="list-style-type: none"> • Accounting for personnel. • Performing essential functions through contingency capabilities. • Coordinating and collaborating. • Establishing communications with interdependent organizations and other internal and external stakeholders. • Submitting any required status updates. 	<ul style="list-style-type: none"> • Establishing that the organization can accomplish all essential functions and operations at the new or restored site. • Phasing down site operations and supervising the return of operations to primary or other operating site using a priority-based approach. • Instructing all personnel on the requirements of new normal operations.

Reconstitution

Reconstitution is the process by which an organization returns to pre-disruption operations and/or establishes a new normal state of operations. It is a phased process for an organization’s resumption of operations or the creation of a new normal that leads to the organization operating differently than it did pre-disruption. Reconstitution occurs in parallel with the continuity of operations efforts.

There are four phases of reconstitution:

- **Readiness & Preparedness**

This phase includes 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 the reconstitution team.

- **Assessment**

The assessment phase is comprised of actions taken immediately following a disruptive event to assess damage and develop courses of action (COAs) for leadership approval.

- **Implementation**

The third phase of reconstitution involves coordination with partners and service providers and the execution of the organization’s approved reconstitution COAs.

- **End of Reconstitution**

Upon return to the site or reestablishment of normal operations, the final phase of reconstitution begins. Hot washes are conducted and AARs are developed, by which plans, procedures, checklists, and agreements are adjusted as needed.

During reconstitution, organizational leadership communicates instructions to all staff and supervises the orderly resumption of normal operations using the primary site and/or systems, temporary sites and/or systems, or new, permanent sites and/or systems. To expedite the return to full and normal operations, reconstitution activities begin before a disruption or threat that leads to the implementation of continuity plans.



The Reconstitution Manager and reconstitution team are critical to reconstitution planning and operations. Organizations are highly encouraged to designate and assign personnel to these roles:

- **Reconstitution Manager**

This individual is responsible for planning, managing, and reporting on the recovery of the organization. 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 (POC) between the organization and other organizations regarding reconstitution issues. Due to the nature of these duties, it is recommended that the Reconstitution Manager not hold the responsibilities assigned to other continuity personnel roles.

- **Reconstitution Team**

Organizations should identify and resource a team dedicated to reconstitution activities. This reconstitution team will be responsible for the development of the pre-event preparedness plan as well as the post-event implementation plan.

Reconstitution can be as simple as communicating to stakeholders that offices and facilities will reopen following limited operations due to a snowstorm and that all employees are expected to report to work for normal operations. Reconstitution can also be as complicated as recovering from the complete destruction of any or all of the continuity planning factors, with challenges that include relocating operations, conducting essential functions with survivors, and identifying and outfitting a new permanent operating site.

The reconstitution of an organization extends beyond rebuilding or acquiring a new physical site. Depending on the incident, an organization may need to address the physical and psychological impacts to personnel, recover records and files, or reacquire specialized equipment to regain full functionality. Planning for reconstitution requires expertise and coordination from the entire organization to ensure a seamless transition back to new normal operations.

Reconstitution activities include, but are not limited to:

- Assessing the status of the affected Staff & Organization, Equipment & Systems, Information & Data, and Sites.
- Determining how much time is needed to repair or restore the affected Staff & Organization, Equipment & Systems, Information & Data, or Sites and/or acquire new staff, equipment, systems, or sites.
- Supervising repairs and restoration activities.
- Assessing the status of staff post-incident to determine their availability to return to work, informing all staff that the actual emergency (or the threat of an emergency) and the necessity for continuity operations no longer exist, and instructing staff on how to resume operations.
- Implementing a priority-based, phased approach to reconstitution.

The information provided in this CGC is a brief overview of reconstitution program management recommendations. Federal partners may also refer to the *FEMA Reconstitution Manager's Guide* for a comprehensive listing and explanation of reconstitution activities.⁶

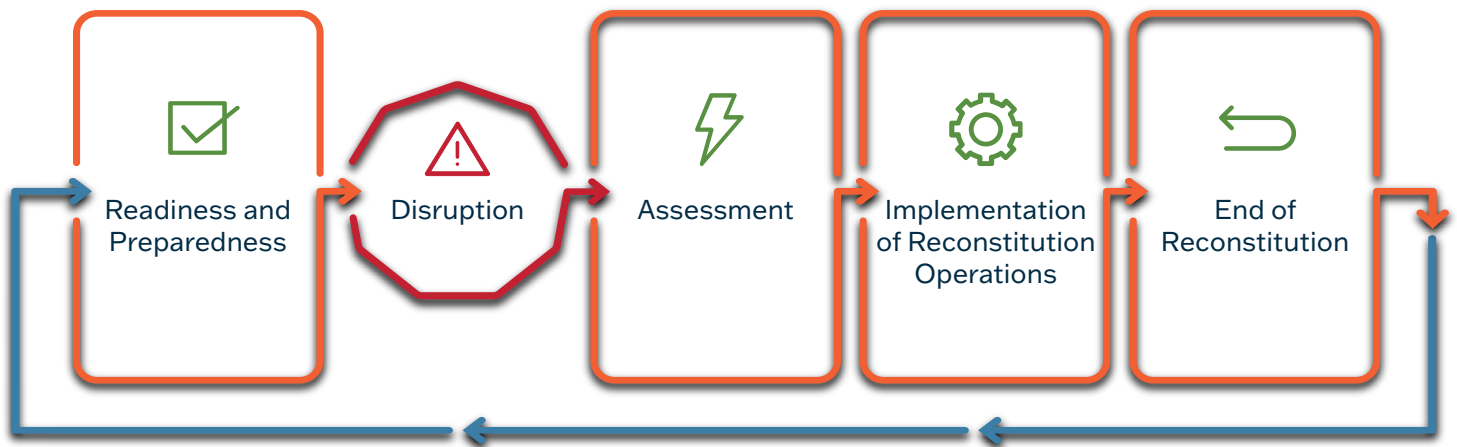


FIGURE 3 | Phases of Reconstitution

⁶ Reconstitution Manager's Guide | FEMA.gov



Chapter 3: Building a Capability

Organizations must fully integrate continuity into all aspects of their daily operations, creating a culture of continuity. This section provides guidance and a framework for building a comprehensive continuity foundation and a plan that is coordinated with partners and stakeholders.

Step 1: Identify Essential Functions

Essential functions are those that must be performed as required, regardless of conditions or circumstances. Essential function identification and analysis require an in-depth understanding of the organization, its foundational mission(s), and how those missions are accomplished.

At the national level, the NEFs are the focus of continuity programs and capabilities before, during, and after a catastrophic emergency. However, the federal government cannot maintain these functions and services without whole of government partnership and community engagement. NEFs are accomplished through a collaborative effort with federal organizations performing various essential functions, integrated and supported by SLTT governments, the private sector, NGOs, and the public. The eight NEFs are shown in Figure 4.

While Federal Executive Branch organizations must identify their essential functions, non-federal entities should identify their own essential functions and align them with the NEFs, as appropriate. Governmental organizations identify essential functions and critical services necessary to accomplish this overarching mission. Other agencies, organizations, and entities—in both the public and private sectors—may also find that their functions are nested within these higher-level essential functions and play a direct role in ensuring the continuation of governmental functions. The following table shows how non-federal essential functions align with the NEFs.

While the NEFs may be one means to identify essential functions, organizations may determine that there are other organizational functions that are essential. Organizational leadership, Mission Owners, and continuity team members, with support from legal counsel, should work together to ensure that every relevant consideration is made.

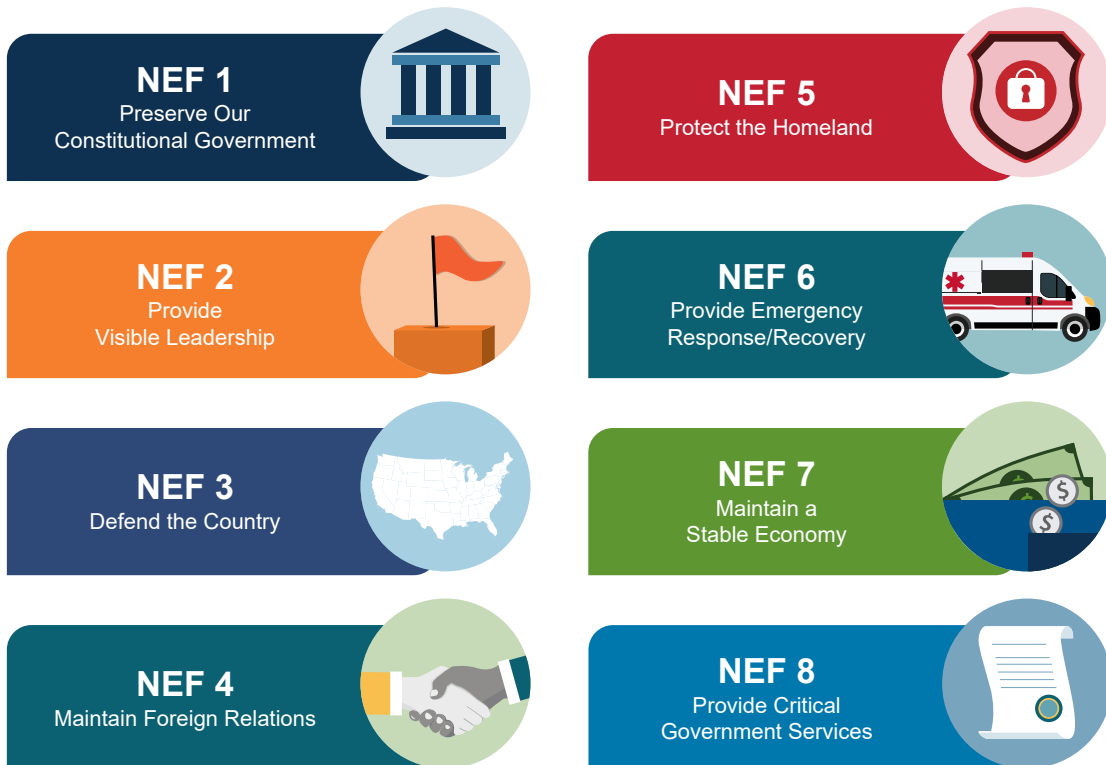


FIGURE 4 | National Essential Functions



TABLE 2 | NEFs and Non-Federal Essential Functions

National Essential Functions	Non-Federal Essential Functions
<p>NEF 1 Ensure the continued functioning of our form of government under the United States Constitution, including the functioning of the three separate branches of government.</p>	<p>Maintain enduring constitutional government, focusing on the continued functioning of critical government leadership elements, including the following: succession to key offices, such as governor, mayor, or parish/local executive; communications within the branches of government, government agencies, and the public; leadership and management operations; situational awareness; and personnel accountability.</p>
<p>NEF 2 Provide leadership visible to the Nation and the world and maintain the trust and confidence of the American people.</p>	<p>Provide visible leadership, focusing on the visible demonstration of leaders effectively dealing with crises and leading response efforts. Essential functions can include monitoring threats and hazards and maintaining the confidence of established government organizations and the public.</p>
<p>NEF 3 Defend the United States against all enemies, foreign and domestic, and prevent or interdict attacks against the United States or its people, property, or interests.</p>	<p>Support the defense of the United States. While the primary responsibility for defending the Nation lies within the federal government, other organizations, such as the National Guard and individuals including tribal citizens, support NEF 3. Numerous organizations and volunteer agencies support individuals in the military. Critical infrastructure and the private sector also play a key role.</p>
<p>NEF 4 Maintain and foster effective relationships with foreign nations.</p>	<p>Maintain and foster effective relationships with neighbors and partners, including maintaining external relationships and agreements with a wide variety of entities. This may vary considerably across states, territories, and Tribal Nations. This includes communications and interactions, as necessary, during a crisis with critical partners and organizations, including the federal government; other SLTT governments; private-sector and nonprofit organizations; and may include foreign governments and organizations. This falls under the umbrella of NEF 4, however, it is recognized that the primary foreign relations responsibility lies with the federal government.</p>
<p>NEF 5 Protect against threats to the homeland and bring to justice perpetrators of crimes or attacks against the United States or its people, property, or interests.</p>	<p>Maintain law and order, focusing on maintaining civil order and public safety, including protecting people, property, and the rule of law; ensuring basic civil rights; preventing crime; and protecting critical infrastructure. A function within this area includes activating National Guard units to support these efforts.</p>
<p>NEF 6 Provide rapid and effective response to and recovery from the domestic consequences of an attack or other incident.</p>	<p>Provide emergency services, focusing on providing critical and accessible emergency services, including emergency management, police, fire, ambulance, medical, transportation, search and rescue, shelters, emergency food services, and recovery operations.</p>



National Essential Functions

Non-Federal Essential Functions

NEF 7 | Protect and stabilize the Nation's economy and ensure public confidence in its financial systems.

Maintain economic stability, focusing on managing the overall local economy. While the federal government is responsible for protecting and stabilizing the national economy and regulating the currency, SLTT governments have a responsibility to manage their jurisdiction's finances, ensure solvency, and ensure that banks, credit unions, savings and loans, and stock and commodity exchanges can open and transact business in accordance with legal obligations, including any power and data services required for transactions. During a crisis affecting the economy, maintaining economic stability and confidence in the financial system is critical at every level of government.

NEF 8 | Provide for federal government services that address the national health, safety, and welfare needs of the United States.

Provide basic essential services, focusing on providing water, power, healthcare (including disability services), personal assistance services, communications, transportation services, sanitation services, environmental protection, commerce, education, and childcare. These services must continue or be restored quickly to provide for basic needs. Other less critical services may be delayed or deferred at the organization's discretion; the focus is on providing those critical services necessary to sustain the population and facilitate establishing a new normal.

Other factors that may inform the identification of an organization's essential functions include the following:

- **Regulatory Compliance**
Identify functions that are necessary for compliance with legal and regulatory requirements. Some activities may be mandated by law and must be maintained to meet legal obligations.
- **Dependency**
Consider the interdependencies between different functions or organizations. Identify functions that support or are supported by others.
- **Stakeholder or Customer Impact**
Assess the impact on stakeholders or customers if specific functions are disrupted.
- **Criticality**
Evaluate functions based on their criticality to the organization's core mission and consider the consequences of disruption on financial, operational, legal, and reputational aspects.

Essential Functions Identification

Not all tasks and activities identified during the Business Process Analysis (BPA), reviewed in Step 2, can be done in a resource-scarce environment. The distinction between essential and nonessential functions is whether an organization must perform a function during disruptions to normal operations or if it can be deferred. If an organization determines that a function may have to continue during or immediately after a disruption to normal operations, it will likely be identified as essential.

While not all identified tasks and activities can be performed in an austere environment, certain functions cannot be discarded. Legally required activities, such as maintaining certain protections—race, color, religion, national origin, age, sex, and disability—are essential. For example, a disruption to normal operations does not mean that an organization can forgo its responsibility to ensure that all programs and services are equally accessible to individuals with disabilities. Critical emergency management activities—such as transportation services, communication, sheltering, and healthcare—must continue to be disability-inclusive.

Although the performance of all functions will eventually need to resume following a disruption, if resources are limited, an organization may have to prioritize some functions over others. Some functions may require continuous performance, while others may be delayed for short periods of time. But even with essential functions, it may be possible to delay resumption for several days.



Several factors should be considered when determining functional criticality, including:

- **Maximum Tolerable Downtime**
How quickly must this task or activity resume if disrupted?
- **Impact if Not Conducted**
What are the impacts of not conducting or delaying the performance of this task or activity? Does this function affect another organization's ability to conduct their essential functions?
- **Management Priority**
What is your organizational leadership's preference and discretion?

Categorizing functions helps organizations prioritize potentially limited resources that their communities will need during and after a disruption to normal operations. Priorities can be fluid and situationally dependent. For example, plowing snow from roads may be an essential function during the winter but not during the summer. The prioritization process will likely involve a combination of both objective and subjective decisions. It may be most efficient to group functions into priority categories rather than attempt to establish a comprehensive linear list. Grouping and prioritizing essential functions in tiers may help the flexibility of an organization in the face of complex incidents.

Additional information on how the Federal Executive Branch identifies and prioritizes essential functions can be found in *FCD: National Continuity Program Management Requirements for the Federal Executive Branch* and *FCD: Identifying and Managing Risk to Essential Functions for the Federal Executive Branch*.

Step 2: Identify Requirements

Conduct a Business Process Analysis

A BPA is a systematic process that identifies and documents the activities and tasks that are performed within an organization. A BPA captures and maps the functional processes, workflows, activities, personnel expertise, systems, resources, controls, data, and sites inherent in the execution of a function or requirement. An effectively conducted BPA supports the development of detailed procedures that outline how an organization accomplishes its mission.

Each organization should look at the BPA process from the point of view of both the overall process flow, including how the organization interacts with partners and stakeholders, and the operational

details. Performing a BPA is not a minor undertaking and should be approached systematically and with a focus on clearly describing the details regarding how each task and activity is performed.

A detailed BPA identifies and answers the following questions:

- What products, services, and information result from the performance of this essential function (including metrics that identify specific performance measures and standards)?
- Who in the organization's leadership is required to make decisions and perform other key actions necessary to ensure the continuity of the essential function?
- What staff are required to directly perform and support the essential function (including specific skill sets, expertise, and necessary security clearance)?
- What equipment and systems, including communications and IT resources, are required to support the essential function (including any unique or unusual requirements)?
- What information and data are required to support the essential function? This is different from the equipment and systems used to store, send, process, or access the information and data because information and data can often be stored, sent, processed, and accessed in multiple ways (e.g., hand delivery of a hard copy of a contact roster or email delivery of a digital copy).
- What are the physical site requirements for performing the essential function (e.g., facility type, square footage, security, infrastructure)?
- What vital mission support activities indirectly accomplish the essential function by enabling or facilitating its performance (e.g., providing a secure workplace, ensuring computer systems are operating)?
- Which external partners perform or provide vital facilitating activities or services that support or ensure essential function performance?
- How is the essential function performed from start to finish?
- What are the budget requirements for performing the essential function and ensuring its continuity during a disruption of normal operations?
- Have the Mission Owners/operators verified that the BPA accurately lists and describes the processes, tasks, Essential Supporting Activities (ESAs), continuity planning factors, and other resources they require to ensure the continuity of their essential function?



The planning factors help organizations assess and address the risks to their essential functions (see Figure 1). These four factors are based on the concept that for operations to occur, **people** must perform activities, **equipment and systems** are used to execute functions, **information and data** are needed to inform decisions, and all these factors exist at both centralized and distributed **sites**.



Staff & Organization

People are the most valuable resource in any organization. Leadership, including Mission Owners as well as management and staff, must be organized to support decision-making and the performance of essential functions.

Organizations should mobilize specific, pre-identified personnel as necessary to sustain essential functions during a disruption to normal operations.

However, all organizational personnel, not just those identified as continuity personnel, should be viewed as resources that should be relied upon. These personnel may be asked to support operations from an organization's alternate site or another directed work location (e.g., alternate worksites, telework, remote work), maximizing workplace flexibilities.



Equipment & Systems

Organizations should plan for every physical resource or digital application resource they require to perform their essential functions. Further, these resources are more resilient when there are redundant options to perform

operations across geographically dispersed locations. The availability of usable computers, servers, software, communications devices, and other physical assets is key to the successful sustainment of essential functions. However, equipment and systems are not exclusively communications or IT-based resources. Physical assets—such as vehicle fleets, aircraft, government vehicles, and forklifts—may also be needed to ensure continuity.



Information & Data

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 an organization's essential functions.

Planning for the resilience of information and data is often unique to each individual system, considering preventative measures, recovery strategies, and technical considerations appropriate to classification level, confidentiality, integrity, and availability requirements. Procedures should be established for personnel to access the information and data they require, regardless of where operations

are occurring. All organizations are responsible for ensuring that third-party data providers provide secure, consistent, and redundant access to networks and data, but they must also account for the loss of commercial services by maintaining and protecting the data stored on their systems. Organizations should plan for the physical loss and degradation of the equipment and systems, or software used to access the data, independent of the loss or degradation of the information and data themselves.



Sites

Primary sites are where organizations perform their day-to-day operations. Organizations should identify alternate sites that are unlikely to be affected by the same disruption or incident that may impact 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 site. Organizations should conduct risk assessments on all operating facilities—primary and alternate—to evaluate the impacts of disruptions caused by threats or hazards on the conduct of essential functions.

In some cases, operations cannot be physically relocated or devolved. For an operation that cannot be duplicated at an alternate site, the best option might be a risk assessment coupled with physical, personnel, communications, and information security measures to harden a site and ensure the resilience of a function. Additionally, hardening may delay the need for an organization to activate continuity plans and provide additional time to coordinate other continuity options.

Step 3: Conduct a Risk Assessment

Risk management is the process of evaluating and communicating risk, as well as accepting, avoiding, transferring, or controlling it to an acceptable level, considering the associated costs and benefits of any actions taken. Effective risk management practices and procedures assist organizations in accomplishing continuity objectives. An organization's risk management program includes continuity of operations as part of its overall risk mitigation efforts.

There are many methods for assessing the potential impacts of threats and hazards and a variety of sources of information on different threats and hazards, including existing assessments, historical records from previous incidents, and analyses of critical infrastructure interdependencies. Risk assessments that entities can



leverage include the Hazard Mitigation Plan's Hazard Identification and Risk Assessment, local site-based Hazard Vulnerability Analyses, cyber and information security assessments, or other risk assessments available at the community or regional level. These risk assessments inform the Business Impact Analysis (BIA) process.

Federal preparedness grant awardees must also submit a Threat and Hazard Identification and Risk Assessment (THIRA) to FEMA and should consider all risk information available to them while developing this assessment. States, territories, major urban areas, and Tribal Nations may use the THIRA process to consider relevant threats and hazards, give them context, and identify their potential impacts. Jurisdictions can then indicate their intended level of preparedness for each of the core capabilities and report which threat or hazard places the greatest potential stress on each capability. FEMA's CPG 201, *Threat and Hazard Identification and Risk Assessment Guide*, outlines the process for conducting a THIRA.

Conduct a Business Impact Analysis

A BIA is a method of identifying and evaluating the effects that various threats and hazards may have on the ability of an organization to perform its essential functions and the resulting impact of those effects. Through the BIA, an organization will identify problem areas (e.g., gaps, weaknesses, and vulnerabilities). In turn, leadership will use the BIA results to make and support risk management decisions. The BIA facilitates the identification and mitigation of vulnerabilities to ensure that when a disruption occurs, an organization can perform its essential functions. The results of the BIA will establish the foundation for evaluating and establishing continuity options to ensure the continued performance of organizational essential functions and the delivery of critical services.

Many methods of conducting BIAs exist, but a comprehensive BIA should answer the following questions:

- Which threats and hazards identified in my risk assessment could plausibly disrupt operations?
- How likely are they to occur?
- What are the strengths and vulnerabilities of each of the four planning factors needed for essential function performance?
- What is the maximum tolerable downtime of a function and associated critical activities before mission failure occurs?
- How is a threat or hazard likely to impact each of the four planning factors, and how likely is it to cause degradation or failure of each?
- What is the overall risk associated with disruption of the essential function's performance?

Organizations should have a strong foundation in all-hazards planning to manage emerging and future risk that is often difficult to anticipate. All-hazards planning recognizes that different threats and hazards often have similar impacts on the four continuity planning factors. These impacts—not the cause of the impacts—are the focus of all-hazards planning. For example, the loss of an essential piece of equipment may be mitigated by having a backup piece of equipment. The cause of the initial loss is not important.

Risk Mitigation Approaches

After organizations have identified and documented the risk to their essential functions, they should take action to manage this risk. Risk management decisions are based on the significance of the risk and what level of risk is deemed acceptable by an organization's leadership. Risk responses may include the following:

- **Acceptance**
No action is taken to respond to the risk based on the insignificance of the risk.
- **Avoidance**
Action is taken to stop the operational process or the part of the operational process causing the risk.
- **Sharing**
Action is taken to transfer or share risk across the entity or with external parties, such as insuring against losses.
- **Reduction**
Action is taken to reduce the likelihood or magnitude of the risk.

Organizations should mitigate unacceptable risk by adopting and employing one or more mitigation approaches and/or continuity options.



Step 4: Identify and Implement Continuity Options

Identifying continuity options to address risks allows organizations to manage those risks with relevant, comparable, and scoped options. Leadership should consider the feasibility of implementing options to support continuity and how alternatives affect and reduce risk. This includes considering resources, capabilities, time to implement, political will, legal issues, the potential impact on stakeholders, and the potential for unintentionally transferring risk within the organization. Organizations may select many strategies to reduce a single vulnerability. For example, if telework is chosen as a primary continuity option, disruptions such as power or communications outages necessitate selecting an alternate continuity option. An alternate or distributed site with resilient communications and backup power capabilities may be a good option.

The continuity options detailed below represent the four core options available to organizations: distribution, devolution, relocation, and hardening. Distributing operations through mobile work, directed work (work performed from directed work locations), and telework may also be leveraged to ensure the performance of essential functions.

Each continuity option has its strengths and weaknesses. Organizations should consider which option is most appropriate to mitigate risk to a particular essential function. Organizations are also encouraged to customize and supplement these options to achieve a robust and resilient capability that ensures essential function performance.

Distribution

Distribution diversifies the continuity planning factors involved in a function's performance. The mixed use of physical and secure cyber capabilities to enhance the availability, integrity, security, and confidentiality of essential functions and activities may include proactive physical relocation outside of a threat area and/or relying on the distribution of capabilities to enhance the resilience of critical infrastructure, vital supply chains, and secure and redundant equipment and systems.

Implementation will look different for every organization depending on factors such as its mission, existing footprint, and resources (including budget), among many others. Organizations should consider that while distribution lowers overall risk, particularly for no-notice events, some residual risk is transferred to other areas.

For example, physically distributing operations will increase reliance on IT equipment and systems to maintain communications and will require investment in additional capabilities to ensure the resilience of the function.

Devolution

Devolution is the transfer of statutory authority and responsibility from an organization's primary operating staff and sites to other designated staff at other sites, using different equipment and systems to sustain essential functions. A continuity plan's devolution option addresses how an organization will identify and transfer organizational command and control, as well as the responsibility for performing essential functions, to personnel at a geographically distributed site unaffected by the incident. Ensuring that appropriate delegations of authority are in place is vital to the success of this option.

This option is not exclusive to organizations with inherently distributed operations, such as regional or field offices. If an incident adversely affects an organization enough that devolution must be initiated, all organizations—no matter the size—may be able to devolve operations to another organization unaffected by the incident. A city could devolve some functions to a neighboring city or to their county. A county or parish could devolve functions to the state or a neighboring county. Devolution is also not a zero-sum option. Organizations may devolve some functions to lighten personnel's overwhelming workload in a resource-scarce environment after an incident.

When planning for devolution, an organization should consider:

- The partner to whom the performance of essential functions will transfer.
- Active and passive triggers that result in the activation and implementation of the devolution plan. Active triggers initiate the devolution option because of a deliberate decision by leadership or elected officials; passive triggers occur when leadership is not available to initiate activation and the devolution partner assumes authority and performs essential functions.
- How and when direction and control of organization operations will transfer to and from the devolution partner.
- The necessary resources—such as personnel, services, equipment, and information—to facilitate the performance of essential functions at the devolution site.



Devolution is a complex continuity option that involves planning and training prior to an incident. The devolution partner should receive training on the following:

- Essential functions and how to conduct them.
- Communications, essential records, and IT systems necessary to perform the essential functions.
- Roles and responsibilities, including how the plan is activated.

Governments should explore whether devolution is a realistic and beneficial option. SLTT governments may be constrained by laws, regulations, licensing, and liability, impacting their ability to devolve certain operations. At a minimum, SLTT governments should pursue mutual aid agreements or MOUs and contracts with private-sector vendors and contractors to supplement or temporarily perform essential functions under the direction and control of the affected jurisdiction.

Mutual Aid Agreements

Jurisdictions at all levels should work with each other to develop mutual aid agreements and procedures. Mutual aid agreements are a NIMS concept. NIMS supports an integrated nationwide network of mutual aid systems at all levels of government and within the private sector. This network enhances resilience by allowing organizations to account for, order, and mobilize outside resources efficiently and effectively. When local and state resources are exhausted, the state sources additional resources through intrastate and interstate mutual aid, such as the Emergency Management Assistance Compact (EMAC), the federal government, or the private sector. The continuity community should consider resources and capabilities across partners and stakeholders and develop written agreements to facilitate access to potentially needed resources.



Relocation

Relocation entails pre-identified members of an organization's primary operating staff moving away from their primary site to continue or resume performance or command and control of essential functions at an alternate site when normal operations are disrupted.

An alternate site should be at a sufficient distance from the primary site that it is unlikely to be affected by the same catastrophic event or emergency that is driving operations from the primary location. When identifying and preparing alternate sites, organizations should maximize the use of existing local infrastructure, such as joint or shared facilities. During the planning stage, organizations should identify alternate sites that are accessible to individuals with disabilities. If none are available, organizations should work with

Depending on the resources available, alternate locations can be classified as one of the following three types:

- 1 | Hot Site** | *An alternate location that is operationally ready with computer systems, telecommunications, and other IT infrastructure. The site can accommodate personnel required to perform essential functions; personnel may or may not be permanently assigned to the location.*
- 2 | Warm Site** | *An alternate location that is equipped with some computer, telecommunications, other IT, and environmental infrastructure that is capable of providing backup after additional personnel, equipment, supplies, software, or customization are provided.*
- 3 | Cold Site** | *A facility that is not staffed on a day-to-day basis by personnel from the primary facility. Organizations may be required to pre-install telecommunication equipment and IT infrastructure upon selection and purchase and deploy designated IT essential personnel to the facility to activate equipment and systems before they can be used.*



facility managers to develop steady-state modifications to the site to ensure readiness during a disruption to normal operations.

Organizations should consider using existing organization space or other space for alternate sites, such as the following:

- **Remote/offsite training facilities**
These facilities may include an organization’s training facility located near the organization’s primary operating site but far enough away to afford some geographical dispersion.
- **Space procured and maintained by another organization**
Some organizations offer space procurement services that other organizations can use for alternate sites.
- **Participation in joint-use alternate sites**
Several organizations may pool their resources to acquire space they can use jointly as an alternate site. With this option, organizations should ensure that the shared facilities are not overcommitted during an activation of continuity plans. An organization may co-locate with another organization at an alternate site, but each organization should have individually designated space and other resources at that site to meet its own needs.
- **Alternate use of existing facilities**
Organizations may use a combination of facilities and methods—such as social distancing in a pandemic scenario, which decreases the frequency and duration of social contact to reduce person-to-person virus transmission—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 accomplishment of essential functions, or if multiple facilities support the accomplishment of a function, activities may be combined as one.
- **Properties owned by Tribal Nations**
Tribal Nations may offer facilities through mutual aid agreements. The properties must be approved for use and cleared by tribal leadership to not have significant cultural value.

Organizations should consider that while relocation may lower overall risk, some residual risk is transferred to other areas. For example, alternate sites may be thoughtfully provisioned and equipped to provide a very resilient option that is appropriate for a wide range of threats and hazards, but the reactive nature of relocation is not well suited to no-notice events. Alternate sites can be expensive to procure and maintain. Organizations may offset some of this cost and residual risk by using the alternate site daily, with a reduced footprint required at the primary site. Organizations are also encouraged to explore shared use possibilities with external organizations.



Telework

When using telework as an option to support essential functions during a disruption to normal operations, organizations should identify which functions can be conducted via telework, including evaluating the use of telework for supporting extended continuity operations and use by non-continuity personnel. Organizations should adhere to relevant laws, statutes, policies, and guidance governing the use of telework; provide protection of information and information systems during telework activities according to established standards; and provide access to essential records and communications necessary to sustain an organization’s essential functions via telework. Organizations should:

- Coordinate with their IT specialists to identify equipment and technical support requirements for personnel identified as telework-capable.
- Work with human resources to support continuing operations in a telework environment.
- Identify necessary, accessible methods to maintain effective communication access and telework for employees who require accommodations.

Telework can assist in the sustainment of essential functions during disruptions such as a pandemic or an incident that causes a building closure. However, telework may not be viable for continuing essential functions during all disruptions to normal operations, such as from the effects of cyberattacks and mass power outages. If an organization plans to use telework to continue essential functions, planners should document this option in its continuity plan. Telework may also not work for all organizations or portions of organizations; the effectiveness of this option will be dependent on factors identified during the BPA. Even if telework may not work for supporting essential functions, it may be an option for supporting functions or capabilities necessary to ensure the continued performance of essential functions.



Hardening

Hardening is the systematic identification and reduction of vulnerabilities found in any of the continuity planning factors. Hardening may involve physical mitigation strategies. While hardening should be used across the four planning factors and to supplement other continuity options, in some instances it is the only continuity options available to help ensure the performance of an essential function. If a function requires a specific piece of equipment or system that cannot easily be reproduced at a different site, or if the function is geographically tied to the site where it is primarily performed, hardening may be the only continuity option available to an organization.

Although hardening should be used as a stand-alone continuity option only when other options are not feasible, it has some advantages. One advantage is that the staff and organization charged with the day-to-day performance of an essential function continue to perform that function at a site and with equipment and systems optimized for that function. Another advantage is that hardening can delay the impacts of a threat or hazard long enough to endure short-term disruptions or find other, ad hoc mitigation solutions. While not specific to the continued performance of essential functions, the adoption of physical mitigation strategies assists organizations in further reducing the risk of disruption to essential functions and services. Physical mitigation strategies that could increase the resilience of an organization and reduce disruption to essential functions include the following:

- Implementing structural changes, such as elevating facilities, floodproofing, or implementing earthquake retrofitting measures.
- Hardening infrastructure, including implementing security measures for facilities, systems, and applications, or rerouting utilities underground.
- Creating redundancy, such as using dual power feeds or an uninterruptible power supply.

Continuity Options by Continuity Planning Factor

Once strategies for mitigating the effects of an incident on the performance of essential functions have been identified, there are a variety of techniques that an organization can use to execute those options. Continuity options serve as the foundation for both how an organization functions during a continuity plan activation and how it functions on a day-to-day basis. Identifying and understanding these elements when there is no active threat or hazard is critical to the continuation of essential functions when an incident occurs.



Staff & Organization

An organization's people are its most valuable resource. Choosing the right people for an organization's staff is always important, and this is especially true in a crisis. Organizations should consider the impact of threats and hazards on the people within their organization. Leadership should set priorities and maintain focus. Some people may have direct roles in an organization's essential functions, while others may have supporting roles, but all are critical to the sustainability of an organization before, during, and after a continuity plan activation. The accomplishment of essential functions is dependent on the safety and social and emotional well-being of an organization's people, including the status of their families, pets, service animals, and homes. Continuity plans should address the needs of the people who work within the organization by building preparedness into the organization's culture of continuity.





Continuity Personnel

Certain personnel within an organization must continue to perform essential functions during and after the continuity activation. Organizations should designate such personnel as continuity personnel and assign backups in the event they are unavailable. These individuals may be required to go to alternate sites or telework during a continuity plan activation to ensure the continued performance of an organization's essential functions.

Organizations should facilitate dialogue among human resources and Continuity Planners when developing continuity plans and programs. Topics to address include the designation of employees as continuity personnel, those who are telework-capable to support continuity operations, and those who may not have an immediate role in operations following a disruptive event but who may be called upon to assist as time progresses.



TABLE 3 | Risk Mitigation by Continuity Planning Factor

 Staff & Organization	 Equipment & Systems	 Information & Data	 Sites
<ul style="list-style-type: none"> • Personnel rosters. • Devolution. • Orders of succession. • Delegations of authority. • Personnel preparedness. • Training. • Geographically distributed personnel. 	<ul style="list-style-type: none"> • Redundancy (backup power; disaster recovery; Primary, Alternate, Contingency and Emergency [PACE] communications options). • Systems hardening (e.g., for solar weather). • Assessments of risks from manufacturers and developers in the equipment and systems supply chain. • Reserve equipment and backup system inventory. 	<ul style="list-style-type: none"> • Printed versions of digital records. • Digital record backups to alternative servers on external networks. • Digital records backed up on digital media storage equipment secured in physical locations. • Data management processes and procedures. • Cybersecurity. 	<ul style="list-style-type: none"> • Site redundancy (e.g., alternate operating sites). • Site distribution (including telework and use of a distributed network of fixed sites). • Mobile operating sites. • Alternate water sources. • Devolution sites. • Physical security measures at primary and alternate sites.

Organizations should develop and implement processes to identify, document, and prepare continuity personnel to conduct or support continuity operations, including the following:

- Explain the expectations, roles, and responsibilities of continuity personnel.

- Inform continuity personnel and alternates, in writing, of their roles and responsibilities, and ensure any applicable collective bargaining obligations are satisfied.
- Maintain an up-to-date roster of both the primary and alternate continuity personnel, including contact information.
- Cross-train personnel to ensure that staffing issues do not affect the organization’s ability to continue its essential functions.
- Advise personnel to maintain family care plans in the event that roles and responsibilities separate personnel from their families for extended periods.



Planning for Personnel with Disabilities

Organizations are responsible for ensuring that continuity planning considers personnel with different types of disabilities, whether hidden or visible. During a disruption to normal operations, the unpredictability and unstable environment may disproportionately impact personnel with certain disabilities. To mitigate this effect, organizations should disseminate continuity plans to personnel in advance of the need to activate the plan. The process for requesting a reasonable accommodation should be fully articulated in the



continuity plan, and organizations should incorporate commonly requested reasonable accommodations into the plan at the outset. Common accessibility categories that should be considered in the continuity plan include the following:

- **Accessible, effective communication.**

Organizations should consider individuals who are deaf or hard of hearing and individuals who are blind or have low vision. Organizations should provide multiple and redundant methods of communication, as one method may not be accessible to everyone. Common accessibility measures include providing captioning on teleconference calls that can be read by personnel who are deaf or are hard of hearing and ensuring that electronic materials are compliant with Section 508, Amendment to the Rehabilitation Act of 1973, so that the materials can be processed by individuals using assistive readers.

- **Accessible facilities and locations.**

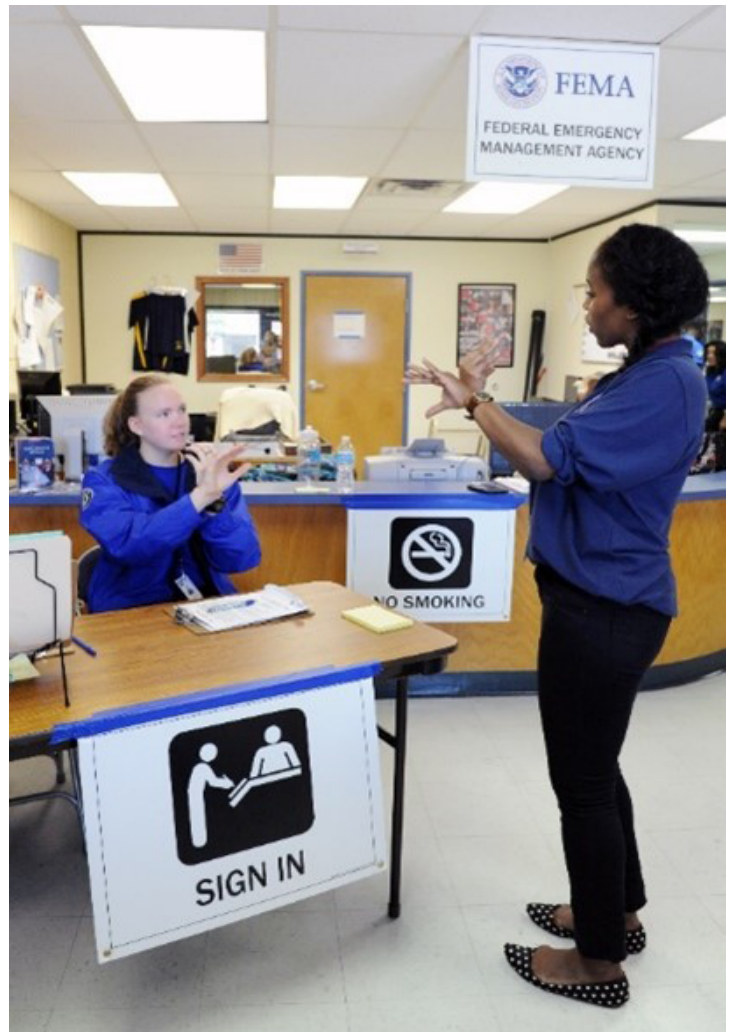
Organizations are responsible for ensuring that the alternate site is accessible to people with disabilities. For people with mobility disabilities, accessibility measures include physically accessible entrances, exits, restrooms, and paths of travel. Also keep in mind that people may require accommodation for disabilities that are unrelated to mobility. For example, people with sensory disabilities, such as those along the autism spectrum, may need a quiet space or room. Having flexibility in the use of the space to make those accommodations is important.

- **Reasonable accommodations or modifications.**

Even when accessibility is included in a continuity plan, personnel have the right to request additional reasonable accommodations or modifications to a program or policy. An organization should have a clearly defined, articulated, and widely advertised reasonable accommodation plan.

Organizations are responsible for supporting non-continuity personnel who may be affected by a disruption to normal operations that causes a continuity plan activation. Organizations should develop a strategy to utilize and support non-continuity personnel during continuity plan activations and operations, which includes the ability to communicate and coordinate with non-continuity personnel and provide guidance on the roles and responsibilities during continuity plan activation and operations.

Personnel accountability is a critical function for all organizations. Organizations should establish procedures to contact all staff—including contractors—in the event of a disruption to normal operations. This enables the organization to communicate and coordinate activities, provide alerts and notifications, and



communicate how and the extent to which employees are expected to remain in contact with the organization.

Orders of Succession

Orders of succession are formal, sequential listings of positions (rather than specific names of individuals) that identify who is authorized to assume a particular leadership or management role when the incumbent resigns or is otherwise unable to perform the functions and duties of their position. Organizations should establish and document, in writing, orders of succession in advance and in accordance with applicable laws to ensure there is an orderly and predefined transition of leadership during any change in normal operations. In some cases, organizations may have the latitude to develop orders of succession, while in other cases, succession is prescribed by organizational structure, statute, order, or directive.

An organization's legal department or equivalent should develop and review the orders of succession to ensure legal sufficiency. Counsel can also address legal issues related to the rules and procedures officials must follow regarding succession, when succession occurs,



the method of notification, and any other limits. Orders of succession positions include, but are not limited to, leadership, elected officials, and key managers. Establishing an order of succession for elected officials or organization heads ensures that a designated official is available to serve as the acting official until appointed by an appropriate authority, replaced by a new permanently appointed official, or otherwise relieved. Organizations should include at least three positions permitted to succeed to the identified leadership position, if possible. In addition, organizations should consider identifying one position within the orders of succession that is typically working in a location that is geographically distributed from the other listed positions.

Delegations of Authority

Delegations of authority ensure the orderly and predetermined transition of responsibilities within an organization and are related to, but distinct from, orders of succession. A written delegation of authority provides the recipients with 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 that authority. Delegations of authority are an essential part of an organization's continuity program and should have sufficient breadth to ensure the organization can perform its essential functions.

An organization's legal department or equivalent should develop and review the delegations of authority to ensure legal sufficiency. Delegations of authority are frequently tied to specific positions, but since many delegations require specific training, qualifications, and certification, organizations must also associate some delegations of authority with specific individuals (e.g., delegations for committing funds, contracting, and technical direction). Organizations should ensure that delegations of authority are identified as essential records, available during a continuity activation and updated on a regular basis.

Delegations of authority should provide details for personnel to make key decisions during emergencies, including the following:

- Outlining explicitly the authority—including any exceptions to that authority—of an official designated to exercise organizational direction.
- Delineating the limits of authority and accountability.
- Outlining the authority of personnel to re-delegate functions and activities, as appropriate.
- Defining the circumstances under which delegations of authority would take effect and be terminated.

Equipment & Systems Communications

The success of continuity programs is dependent on the availability of and access to communications systems with sufficient resilience, redundancy, and accessibility to perform essential functions. During a disruption to normal operations, an organization's ability to execute its essential functions at its primary or alternate site depends on the availability of communications systems. These systems support connectivity among key leadership, internal elements, other organizations, and the public under all conditions.



External communications during a continuity plan activation are an essential function of many organizations during emergencies. External stakeholders and the public will expect information to flow from an affected area. It is vital that the organization can communicate its status and quickly provide additional effective information that is accurate and accessible to the whole community, including individuals with disabilities.

Organizations should integrate communications contingency needs into continuity planning efforts by incorporating mitigation options to ensure uninterrupted communications support. The risk assessment and BIA identify risks to primary and alternate communications systems involved in the performance of essential functions, which are identified during the BPA. For example, organizations can incorporate diverse and redundant communication lines into their facilities, ensure that communications equipment (e.g., switches or power distribution units) has strategic sparing of single points of failure, and confirm the geographic separation of primary and alternate transmission media.

Communications capabilities should be interoperable, robust, redundant, and secure to enable any communications involving



sensitive and classified information. They should also be diverse and available in sufficient quantity and mode/media, commensurate with each organization's responsibilities in response to a given disruption. Organizations should establish a cybersecurity plan that includes continuity of a communications component such as radio frequency-based communications that do not rely on public infrastructure.

Organizations should adequately maintain communications capabilities and train personnel required to use them. If alternate sites, devolution, mutual aid agreements, or other mitigation measures are used, organizations should ensure adequate access to and interoperability between communications resources. This includes confirming that current copies of essential records, including electronic files and software, are backed up and maintained off-site.



Potential backup communications options include the following:

- **Radio**, including high-frequency and amateur ham radio. Amateur ham radio operators have proven their ability to coordinate and communicate during emergencies. States and territories also have access to the FEMA National Radio System (FNARS), a backup to commercial telecommunications and messaging capabilities, independent of but interoperable with normal communications systems.
- **Satellite systems**. Satellite-based platforms offer voice, video, and data capabilities should terrestrial communications

fail or for use at locations less likely to be served by terrestrial systems, such as wired or cellular networks.

- **Wireless Priority Service (WPS)**. The WPS supports national leadership, federal and SLTT governments, and other authorized national security and emergency preparedness users. It is intended to be used in an emergency or crisis when the wireless network is congested and the probability of completing a normal call is reduced. The WPS provides personnel priority access and prioritized processing in all nationwide and several regional cellular networks, greatly increasing the probability of call completion.
- **Government Emergency Telecommunications Service (GETS)**. The GETS provides a similar service as WPS. The GETS provides emergency access and priority processing in the local and long-distance segments of the Public Switched Telephone Network (PSTN). It is intended to be used when the PSTN is congested and the probability of completing a call is significantly reduced.
- **Telecommunications Service Priority (TSP)**. The TSP is a program that authorizes national security and emergency preparedness organizations to receive priority treatment for vital voice and data circuits or other telecommunications services.

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

The Cybersecurity and Infrastructure Security Agency (CISA) administers and supports the SAFECOM program, which continuously works to improve emergency response providers' interjurisdictional and interdisciplinary emergency communications capability, interoperability, and security across SLTT, regional, and international borders. It also enables emergency responders, along with the federal government, to communicate through different communication systems to exchange information. SAFECOM has resources available from the National Council of Statewide Interoperability Coordinators and the Federal Partnership for Interoperable Communications on topics relevant to emergency response communications, including guidance on applying for federal financial assistance funding to invest in emergency communications projects.



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. Often monitored concurrently with primary means. Examples include mobile telephone, voice, and data.



CONTINGENCY

This method will not be as fast, easy, inexpensive or convenient as the first two methods but can accomplish the task. Without pre-coordination, however, the receiver rarely monitors this method. Examples include satellite telephone, voice, and data.



EMERGENCY

Method of last resort that typically has significant delays, costs, and/or impacts. Often monitored only when the other methods fail. One example is a mobile radio system.

FIGURE 5 | PACE Model

Critical Systems

In compiling a detailed BPA, an organization will identify various tasks, functions, and systems that are important for the continuation of essential functions. These systems go beyond communications and information systems and may include specialized equipment and systems.

Continuity planning is often unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to each system's information confidentiality, integrity, and availability requirements, as well as the system's impact level. Organizations should account for and utilize various mitigation options for systems (including those outlined in

an IT/DR plan) that support the organization's operations and assets, including those provided or managed by another organization, contractor, or other source.

IT is the foundation of many tasks, activities, functions, and capabilities; it is used every day. People rely on IT for communications and records access, among various other services. However, despite the criticality and the universal nature of IT, it is not the sole focus of continuity. When coordinating IT/DR and continuity plans, the priorities and recovery time objectives for IT capabilities, systems, and services identified during the BPA and BIA processes should be incorporated into the overall continuity plan. Because technology is continuously evolving, organizations should regularly review systems and processes to ensure that their plans keep up with current technology.

A High Value Asset (HVA) is 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 serious impacts to the organization's ability to perform its mission or conduct business. CISA provides resources for organizations to counter dynamic threats to the security or resilience of HVAs.

Information & Data

Essential Records

All organizations create and manage large volumes of information and data, both in electronic and physical form. Some of that information and data are essential to the survival and continued operations of the organization. The information and data needed





to ensure the continuation of essential functions should be pre-identified, protected, and backed up. The impact of data loss or corruption from hardware failure, human error, hacking, or malware could be significant. A plan for data backup and restoration of electronic information is vital and should be done jointly and coordinated with both the overall continuity plan and the IT/DR plan.

Electronic and hard copy documents, references, and records needed to support essential functions during a continuity plan activation are categorized as essential records. The following are examples of essential records:

- Standard operating procedures.
- Continuity plan and other EOPs.
- Personnel and payroll records.
- Contracts.
- Vendor agreements.
- MOAs/MOUs.
- Tribal legal documents.
- Orders of succession.
- Delegations of authority.

Viable continuity programs include comprehensive processes for identifying, protecting, and accessing electronic and hard copy essential records at primary and alternate sites. Organizations should standardize redundant data management software applications and equipment throughout the organization. They should also provide the appropriate level of access and cybersecurity measures to protect sensitive and personally identifiable information, as well as adhere to applicable requirements, such as those covered under the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act (HIPAA). Options for ensuring access to essential records during an incident that disrupts normal operations include the following:

- **Using Backup Servers**

Data and records are backed up on a secondary server, in addition to the primary server. Organizations with a backup server stored in a location different from the primary facility increase the possibility that data, records, and systems are available and accessible.

- **Pre-Positioning Hard Copy Records**

Printing hard copies of records ensures an organization is not reliant on electronic equipment to access records. Pre-positioning copies at alternate sites further protects an organization should the primary site become inaccessible.

Essential records are defined as “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**).”

Emergency Operating Records

Records and electronic information systems essential to the continued functioning or reconstitution of an 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 an 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 an 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 execution 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 that are 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 site.



- **Leveraging Cloud Computing**

In cloud computing, remote servers hosted on the internet are used to store, manage, and process data. This disperses risk to an organization as data is not hosted on local servers, provided that the cloud service provider also has adequate continuity plans.

Regardless of their size, organizations should implement strategic decisions that improve cybersecurity posture and take steps to reduce the likelihood of a damaging loss of information. Organizations should have multiple copies of their essential records in several locations stored on redundant media and in virtual storage environments. Organizations may consult resources provided by the National Archives and Records Administration (NARA) for information about essential records and records recovery after a disaster. Hardening measures to protect the organization’s data—such as data redundancy, encryption, and strict access controls—should be implemented to mitigate risks that may impact the performance of essential functions. These actions should apply to physical servers that house critical information and data, as well as software, applications, and networks. Taking these steps will enable an

organization to quickly detect a potential intrusion and ensure that it is prepared to respond and protect its most critical assets against a disruptive cyber incident.

Lastly, organizations should improve their cyber resilience through deliberate cybersecurity risk management activities. CISA urges cybersecurity/IT personnel to regularly review organizational threats and destructive exploits against critical infrastructure. CISA’s Shields Up campaign provides recommendations, products, and resources to increase organizational vigilance and keep stakeholders informed about cybersecurity threats and mitigation techniques. The complementary Shields Ready campaign provides guidance for critical infrastructure organizations to identify critical assets, map dependencies, develop plans and exercise capabilities, and implement program evaluation and improvement activities to reinforce readiness. The National Institute of Standards and Technology (NIST) has also published a cybersecurity framework, which provides a methodology for organizations to improve their cybersecurity posture and manage cybersecurity risk.





Chapter 4: Maintaining a Capability

After building a continuity program and plan, organizations should continue to maintain and improve that capability. As living documents, plans and policies should be continuously updated and refined. This section provides guidance and a framework for maintaining a viable continuity capability and maturing a continuity program and plan.

Technical Assistance and Training

Technical assistance and training with internal and external stakeholders familiarize individuals with roles, responsibilities, plans, and procedures for conducting essential functions and providing critical services when normal operations are disrupted. Technical assistance and training activities should be based on clear and relevant objectives that are specific to the audience. Organizations should seek opportunities to integrate continuity training with other organizational technical assistance and training activities.

Organizations should train on:

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

Evaluation

Evaluation activities assess and validate continuity plans, policies, procedures, and systems. An evaluation of capabilities includes the use of testing and exercising. Conducting an evaluation using an all-hazards approach—using threats, hazards, and vulnerabilities identified through organizational risk assessments—affirms the viability of continuity plans and programs. Integrated and coordinated events in which whole community partners participate will further help to sustain COG and ECG. To the extent possible, organizations should incorporate continuity aspects into their organization-wide evaluation program rather than develop and conduct stand-alone continuity evaluation activities. Some communities may be completing a THIRA and using the data from this process to assess their capabilities in the Stakeholder Preparedness Review (SPR) to identify capability gaps relating to the POETE solution areas. Integrating continuity considerations into the conduct of THIRA/SPR allows for further integration of continuity into overall organizational resilience.

Testing

Testing demonstrates the correct operation of all equipment, procedures, processes, and systems that support an organization's continuity program. This ensures that resources and procedures are kept in a constant state of readiness. As detailed in FCD: *National Continuity Program Management Requirements for the Federal Executive Branch*, testing and exercising an organization's policies, plans, and procedures cultivates better organizational knowledge, identifies gaps in coverage, and validates existing plans and programs.

Organizations should test:

- Alert and notification systems and procedures for all employees and continuity personnel.
- Protection, access, and recovery strategies found in continuity and IT/DR plans for essential records, critical information systems, services, and data.
- Internal and external interoperability and functionality of primary and backup communications systems.





- Backup infrastructure systems and services, such as power, water, and fuel.
- Other systems and procedures necessary to the organization's continuity option(s), such as the IT infrastructure required to support telework options during a continuity plan activation.
- Measures to ensure accessibility for employees and members of the public with disabilities.

- Internal and external interdependencies, including support for essential functions and services and situational awareness.
- Recovery from the continuity plan activation and environment and transition to establish a new normal.

Continuous Improvement Planning

Documenting the strengths, areas for improvement, and associated corrective actions reinforces continuity preparedness and helps organizations build capabilities as part of a larger continuous improvement process. Over time, exercises should yield observable improvements in readiness and preparedness for future exercises and real-world incidents.

Organizations should incorporate evaluations, AARs, and lessons learned into the development and implementation of an improvement plan. The corrective actions identified during individual exercises, real-world incidents, and assessments should be tracked to completion, ensuring tangible improvements in capabilities. An effective corrective action program develops improvement plans that are dynamic documents that are continually monitored and implemented as part of the larger system of improving preparedness across the organization.

Updating and Reviewing Plans and Programs

A plan is a continuous, evolving document that maximizes opportunities and guides operations. Since planning is an ongoing process, a plan is a product based on information and understanding at that time and is subject to regular—ideally annual—review and continuous revision.

Plan Revision Cycle

Organizations should periodically review and revise their continuity option(s), plan, and supporting documentation and agreements, including mutual aid agreements and MOUs/MOAs. A cyclical model of planning, training, evaluating, and implementing corrective actions provides leaders and personnel with the baseline information, awareness, and experience necessary to fulfill continuity program management responsibilities. Objective evaluations and assessments, developed from tests and exercises, provide feedback on continuity planning, procedures, and training. This feedback supports the corrective action process, which helps to establish



Exercising

Exercises play a vital role in preparedness by enabling partners, stakeholders, and elected officials to shape the planning, testing, and validation of plans and capabilities, as well as identify and address gaps and areas for improvement. Exercise activities improve an organization's preparedness posture and emphasize the value of integrating continuity functions into daily operations. Exercises provide a low-risk environment to test capabilities, familiarize personnel with roles and responsibilities, and foster meaningful interaction and communication across organizations.

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

Organizations should exercise:

- Continuity plans and procedures to validate the organization's ability to continue its essential functions and services.
- Intra- and interagency backup communication capabilities.
- Backup data and records required to support essential functions for sufficiency, completeness, currency, and accessibility.



priorities, inform budget decision-making, and drive improvements to plans and procedures as they are revised.

Several factors may affect how often and when an organization or level of government updates its continuity option(s) and plan:



Change in leadership. New leadership may want to revise policy, plans, and procedures based on their priorities, experience, and history. Newly elected officials and changes to leadership will require updates to orders of succession and delegations of authority.



Organizational realignment or reorganization. An organizational realignment or reorganization may result in changes to essential functions. Rosters, essential records, and other information may then need to be revised.



Change in process or system that supports the function. Continuous updates and changes to processes or systems are vital to ensuring the seamless functionality of requirements to enhance functionality.



Results of individual exercises, tests, and disruptions to normal operations. Effective evaluation involves planning for as well as collecting data during training, testing, exercises, and real-world disruptions, then analyzing the data and reporting outcomes.

Addressing these shortcomings often requires updating plans and procedures.



Mandated requirements. Organizations, governments, and industry standards may set requirements for revision and maintenance schedules. For example, *FCD: National Continuity Program Management Requirements for the Federal Executive Branch* outlines annual and

biennial continuity program maintenance requirements for Federal Executive Branch organizations.

Continuity Metrics

The purpose of developing a continuity capability is to ensure that an organization can perform its essential functions and provide critical services no matter the disruption. Organizations develop continuity metrics and then evaluate and assess continuity plans and programs against these metrics to determine the program's viability.

Evaluations and assessments help organizations identify areas of strength, areas for improvement, best practices, and lessons learned so that they can better prioritize and address resource continuity needs and gaps.

Key continuity metrics measure an organization's ability to perform its essential functions and be operational during a continuity plan activation. Requirements and standards found in continuity regulations or policies can serve as continuity metrics. Tests and exercises serve as valuable tools for measuring progress against metrics.

The Continuity Assessment Tool (CAT) provides a tool for non-federal agencies to assess their continuity capability against the requirements for a viable continuity program and plan as outlined in this document. The sections of the CAT correspond to the sections of this circular. Each section includes continuity activities and supporting tasks critical to that section. These supporting tasks are further divided according to the five POETE solution areas found in the SPR. Through this format, an organization can identify its overall progress toward achieving the recommendations for building a viable continuity capability as outlined in this document. The CAT is found in the Continuity Resource Toolkit and should be used on a regular (e.g., annual, multiyear) basis as a method for determining whether gaps exist in the agency's continuity program and plan.

Resource Direction and Investment

People, communications, facilities, infrastructure, and transportation resources are necessary for the successful implementation and management of an organization's continuity program. Organizations should align and allocate the resources needed to implement their continuity option(s). Through the budgeting and planning process, an organization's leaders and staff ensure the availability of critical continuity resources needed to continue the performance of the organization's essential functions before, during, and after a disruption.

Once an organization has identified its continuity option(s)—including identifying essential functions, conducting a risk assessment, and identifying mitigation and continuity options—it must budget for its continuity activities before, during, and following a continuity plan activation.

- **Before a continuity plan activation**

Organizations should budget for continuity resources and requirements identified during the readiness and preparedness phase, including communications equipment, infrastructure,



and training and evaluation events. For example, exercises may require travel and overtime costs.

- **During a continuity plan activation**

Organizations should acquire and procure equipment, supplies, and resources not already in place that are needed to sustain operations. For example, activation of an emergency contract may require funding.

- **Following a continuity plan activation**

Establishing a new normal may require funding as well as addressing areas for improvement. For example, if the organization used generator fuel during continuity operations, it must fund refilling the supply.

In an era of declining budgets, organizations can identify avenues to fund continuity planning, equipment, and initiatives:

- **Explore grant funding.**

Continuity planning is an allowable use of funding under the Homeland Security Grant Program (HSGP) and Emergency Management Performance Grant (EMPG). Tribal governments may use the competitive grant process through the Tribal HSGP. Each government agency sets its priorities for the use of grant funding under these programs. Planners and organizations should contact their jurisdiction's grant funding program for additional information and to determine if continuity needs will qualify.

- **Identify dual-use technology and resources.**

The acquisition and upgrade of equipment or systems can benefit an organization's continuity capability if considered and planned for accordingly. For example, when agency computers are due for replacement, replacing desktop computers with laptops can enable an organization's flexibility and distribution capabilities. Similarly, upgrades or purchases of some continuity equipment benefit the entire organization; therefore, the cost should be shared by the whole organization rather than just one program.

- **Leverage low- or no-cost resources.**

FEMA offers free continuity training, tools, and templates. Virtual training—such as internet-based courses or webinars—also provides a low-cost alternative. Teaming with other organizations through mutual aid agreements, EMAC, or MOUs/MOAs are low-cost methods of enhancing capabilities.

Multiyear Strategic Planning

Multiyear planning is a useful strategy to develop and improve continuity programs. Organizations should develop a multiyear strategic plan for continuity that provides for the development, maintenance, and review of continuity plans to ensure the program remains viable and successful. This strategic plan should outline the following:

- Short-term and long-term goals and objectives for the continuity option(s) and program.
- Issues, concerns, and potential obstacles to implementing the continuity program, as well as a strategy for addressing them, as appropriate.
- Planning, training, and evaluation activities, as well as milestones for accomplishing these activities.
- Resource requirements to support the program, including funding, personnel, infrastructure, communications, and transportation.

Organizations should link and integrate their continuity budget directly with the objectives and metrics set forth in the strategic plan.





Conclusion

Individuals, communities, organizations, the federal government, and non-federal governments at all levels play a key role in ensuring a resilient nation by providing critical services and conducting essential functions daily. When a disruption to normal operations occurs, the need for these services and functions becomes even more critical. Therefore, governments and organizations need plans to ensure the performance and provision of these functions and services to overcome the challenges posed by the disruption.



The right people, the right resources, and the right planning help ensure the continuous performance of essential functions. Continuity cannot be an afterthought. Unfortunately, natural hazards and human-caused threats can interrupt the functions of government and private-sector organizations. Some of these threats are more predictable than others. Hurricanes, ice storms, flooding, tornadoes, and pandemic outbreaks may or may not allow for a warning period prior to their arrival. Other hazards—such as earthquakes, accidents, sabotage, and terrorism, which are not as predictable—may occur suddenly and with little or no warning. These threats are real, dangerous, and could adversely affect the ability of government at all levels and the private sector to provide essential functions and

services to the Nation. Thus, there is a critical and ongoing need for organizations to ensure the effectiveness of continuity capabilities through planning, operations, tests, training, and exercises. In doing so, the whole community continues to build toward the vision of a more resilient nation through the integration of continuity plans and programs within government and NGOs to sustain national essential functions under all conditions.



Annex A: Continuity Program Guidance

GETTING STARTED

- [] Examine the current state of the organizational continuity program.
- [] Identify the organization's current and potential partnerships within the community, which are critical to developing and sustaining a culture of continuity.
- [] Identify existing coordinating structures in which organizational continuity planners should participate to integrate continuity planning, operations, and responsibilities into emergency management, preparedness, and resilience efforts.
- [] Identify and coordinate with other inter- and intra-organizational continuity plans and programs (e.g., incident management, occupant emergency plans, emergency operations plans, IT/Disaster Recovery Plans) to ensure synchronization across plans and programs.

INITIATING PLANNING

- [] Examine the current state of the organizational continuity program.
- [] Establish a continuity planning team to assist with planning, including representatives from other organizational offices or departments.
- [] Develop a project plan, timelines, and milestones.
- [] Identify preliminary budgeting and resource requirements.
- [] Create an overall strategy to establish a continuity program that is agreed upon by elected officials and organizational leadership, including Mission Owners.
- [] Identify continuity program roles and responsibilities.
- [] Obtain the support of leadership and elected officials for the continuity program.
- [] Review Comprehensive Preparedness Guide 201, *Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide*.
- [] Identify the organization's current and potential partnerships within the community, which are critical to developing and sustaining a culture of continuity.
- [] Identify the organization's essential functions and essential supporting activities by determining what organizational functions are essential, considering statutory requirements and linkages to National Essential Functions and other essential functions in the community.
- [] Outline a continuity plan that accounts for the four phases of continuity and reconstitution.

BUILDING A CAPABILITY

- [] Conduct a Business Process Analysis (BPA) to identify and document the activities and tasks that are performed within an organization, capturing and mapping the functional processes, workflows, activities, personnel expertise, systems, resources, controls, data and facilities, and IT/DR inherent in the execution of each essential function.
- [] Conduct a Business Impact Analysis (BIA) to identify and evaluate how the organization's threats and hazards may impact the organization's ability to perform its essential functions.
- [] Conduct a risk assessment to identify and analyze potential threats and hazards.



- [] Identify mitigation options to address the risks identified in the BIA (e.g., alternate operating facilities, telework policies, devolution procedures, mutual aid agreements).
- [] Identify the organization's key elements (e.g., technology, people), and detail how those elements support the execution of essential functions.
- [] Draft a comprehensive plan that outlines the requirements and procedures needed to perform essential functions and establishes contingency plans if key resources are not available.

MAINTAINING A CAPABILITY

- [] Establish a schedule for conducting regular training and evaluation events to assess and validate continuity plans, policies, procedures, and systems.
- [] Create a corrective action program to implement and track areas for improvement identified during tests, exercises, or real-world incidents.
- [] Develop continuity metrics and success criteria against which to evaluate and assess the organization's continuity plans and program.
- [] Establish a schedule for conducting a review (using the continuity metrics and success criteria) and revision of the organization's continuity option(s), plan, and supporting documents and agreements, such as memoranda of understanding/agreement (MOUs/MOAs).
- [] Align and allocate resources (e.g., budget) to implement continuity activities before, during, and after a continuity activation.
- [] Develop a multiyear strategic continuity plan to provide for the development, maintenance, and review of continuity capabilities to ensure the program remains viable and successful, including training and evaluation activities and plan reviews.



Annex B: Authorities and References

AUTHORITIES

- 01 Homeland Security Act of 2002, as amended (6 U.S.C. § 101 et seq.).
- 02 National Security Act of 1947, as amended (50 U.S.C. § 3042).
- 03 Telework Enhancement Act of 2010 (5 U.S.C. §§ 6501–6506).
- 04 Executive Order 12148, Federal Emergency Management, July 20, 1979, as amended.
- 05 Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities*, November 18, 1988.
- 06 Executive Order 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, July 6, 2012.
- 07 Presidential Policy Directive 8, *National Preparedness*, March 30, 2011.
- 08 Presidential Policy Directive 40, *National Continuity Policy*, July 15, 2016.
- 09 National Security Memorandum 22, *Critical Infrastructure Security and Resilience*, April 30, 2024.

REFERENCES

- 01 Comprehensive Preparedness Guide (CPG) 101, *Developing and Maintaining Emergency Operations Plans*, Version 3, November 2021.
- 02 CPG 201, *Threat and Hazard Identification and Risk Assessment (THIRA) and Stakeholder Preparedness Review (SPR) Guide*, Third Edition, May 2018.
- 03 Federal Continuity Directive, *Continuity Planning Framework for the Federal Executive Branch*, December 2023.
- 04 Federal Continuity Directive-1, *Federal Executive Branch National Continuity Program and Requirements*, January 2017.
- 05 Federal Continuity Directive-2, *Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process*, June 2017.
- 06 DHS, *Homeland Security Exercise and Evaluation Program (HSEEP)*, January 2020.
- 07 FEMA, *National Incident Management System (NIMS)*, October 2017.
- 08 FEMA, *National Preparedness Goal*, September 2015.
- 09 Health Insurance Portability and Accountability Act.
- 10 Privacy Act of 1974.



Annex C: Definitions

Activation | The implementation of a continuity plan, in whole or in part.

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 (WMD), and chemical, biological (including pandemic), radiological, nuclear, or explosive (CBRNE) events (Source: Federal Emergency Management Agency [FEMA]).

Alternate Sites | Fixed, mobile, or transportable sites, other than the headquarters facility, where department and agency leadership and continuity personnel relocate to perform essential functions following activation of the continuity plan. These locations include sites where telework and remote work occur (Source: FEMA).

Business Impact Analysis (BIA) | A method of identifying the consequences of failing to perform a function or requirement.

Business Process Analysis (BPA) | A method of examining, identifying, and mapping the functional processes, workflows, activities, personnel expertise, systems, data, interdependencies, and alternate locations inherent in the execution of a function or requirement.

Continuity | The ability to provide uninterrupted services and support while maintaining organizational viability before, during, and after an incident that disrupts normal operations (Source: FEMA).

Continuity Capability | The ability of an organization to continue to perform its essential functions using continuity of operations, continuity of government (COG) programs, and continuity requirements that have been integrated into the organization's daily operations. The primary goal is preserving our form of government under the U.S. Constitution and the continued performance of National Essential Functions (NEFs) under all conditions (Source: FEMA).

Continuity Coordinator | A senior accountable official, designated by leadership or elected officials, who is responsible for oversight of the continuity program. Continuity Coordinators are supported by a Continuity Program Manager and other Continuity Planners within subcomponent levels throughout the organization or government.

Continuity of Government | A coordinated effort within the executive, legislative, or judicial branches to ensure that essential functions continue to be performed before, during, and after an emergency or threat. Continuity of government is intended to preserve the statutory and constitutional authority of elected officials at all levels of government across the United States.

Continuity of Operations | An effort within individual organizations to ensure that essential functions continue to be performed during a disruption to normal operations.

Continuity Personnel | Those personnel who provide organizational leadership with advice, recommendations, and functional support necessary for the continued performance of Mission Essential Functions (MEFs) (Source: FEMA).

Continuity Plan | A documented plan that details how an individual organization will ensure it can continue to perform its essential functions during a wide range of incidents that impact normal operations.

Continuity Planner | The person responsible for developing and maintaining an organization or subcomponent continuity plan and integrating and coordinating the continuity plan with broader organizational or governmental guidance, requirements, and initiatives.

Continuity Planning Team | The continuity plan impacts the entire organization and requires input from various offices. The continuity planning team is comprised of these offices that assist the continuity program and planning effort.



Continuity Program Manager | The senior Continuity Planner responsible for coordinating overall continuity activities within the organization or jurisdiction. This individual manages day-to-day continuity programs, coordinates with Continuity Planners within the organization, represents his/her organization's program externally, as appropriate, and reports to the Continuity Coordinator on continuity program activities.

Crisis Action Team | A team of senior leadership and/or subject matter experts who review the situation and determine if the continuity plan should be activated.

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

Enduring Constitutional Government (ECG) | A cooperative effort among the executive, legislative, and judicial branches to preserve the constitutional framework under which people are governed. Enduring constitutional government focuses on the ability of all three branches of government to execute constitutional responsibilities, provide for orderly succession and appropriate transition of leadership, and provide for interoperability and support of essential functions during a catastrophic emergency.

Essential Functions | A subset of organizational functions that are determined to be critical activities. These essential functions are then used to identify supporting tasks and resources that must be included in the organization's continuity planning process.

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

Exercise | An event to train for, assess, practice, and improve continuity capabilities in a risk-free environment.

Federal | Of or pertaining to the Federal Government of the United States of America.

Hazard | A natural, technological, or human-caused source or cause of harm or difficulty.

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.

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.

Jurisdiction | A range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographical (e.g., federal, state, tribal, or local boundary lines) or functional (e.g., law enforcement, public health).

Local Government | Public entities responsible for the security and welfare of a designated area as established by law. "(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 entity, or in Alaska a Native Village or Alaska Regional Native Corporation; and (C) a rural community, unincorporated town or village, or other public entity" (Source: 42 U.S.C. § 5122 [8]).

Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) | A written agreement between organizations that requires specific goods or services to be furnished or tasks to be accomplished by one organization in support of the other.

Mission Owner | An individual accountable for performing an essential function that must be sustained during or quickly resumed following a disruption to normal operations. This is the senior accountable position with the original or delegated authority to lead the planning, budgeting, accomplishment, and associated risk management of a specific essential function (Source: FEMA).



Mitigation | Activities providing a critical foundation in the effort to reduce the loss of life and property from natural and/or human-caused disasters by avoiding or lessening the impact of a disaster and providing value to the public by creating safer communities.

Mutual Aid Agreement | A written or oral agreement between and among agencies/organizations and/or jurisdictions that provides a mechanism to quickly obtain emergency assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate rapid, short-term deployment of emergency support prior to, during, and/or after an incident.

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, in order to ensure the preservation of our form of government under the Constitution and the continuing performance of NEFs under all conditions (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.

National Incident Management System (NIMS) | A systematic, proactive approach guiding government agencies at all levels, NGOs, and the private sector to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, to reduce the loss of life or property and harm to the environment.

Nongovernmental Organization (NGO) | An entity with an association that is based on the interests of its members, individuals, or institutions. It is not created by a government, but it may work cooperatively with the government. Such organizations serve a public purpose, not a private benefit. Examples of NGOs include faith-based charity organizations and the American Red Cross. NGOs, including voluntary and faith-based groups, provide relief services to sustain life, reduce physical and emotional distress, and promote the recovery of disaster victims. These groups often provide specialized services that help individuals with disabilities. NGOs and voluntary organizations play a major role in assisting emergency managers before, during, and after an emergency.

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.

Prevention | The capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. For the purposes of the prevention framework, the term “prevention” refers to preventing imminent threats.

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

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.

Protection | The capabilities necessary to secure the homeland against acts of terrorism and human-caused or natural disasters.

Reconstitution | The process by which surviving and/or replacement organization personnel resume normal operations.

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.

Redundancy | The state of having duplicate capabilities, such as systems, equipment, or resources.

Response | The capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.

Risk | The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. With respect to continuity, risk may degrade or hinder the performance of essential functions and affect critical assets associated with continuity operations.

Risk Analysis | A systematic examination of the components and characteristics of risk.



Risk Assessment | A product or process that collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision-making.

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.

Telework | A flexible work arrangement under which an employee performs the duties and responsibilities of their position and other authorized activities from an approved worksite other than the location from which the employee would otherwise work.

Test | The use of quantifiable metrics or expected outcomes to validate the operability of one or more IT systems or system components that are identified as critical in an IT plan.

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.

Training | Effort to provide organizational staff with the knowledge, skills, and abilities needed to perform key tasks required to accomplish specific continuity capabilities.

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 Alaskan Native Claims Settlement Act (85 Stat. 688 [43 U.S.C.A. and 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.

Whole Community | The whole community is an inclusive approach to emergency preparedness and management through the inclusion of individuals and families, including those with access and functional needs; businesses; faith-based and community organizations; nonprofit groups; schools and academia; media outlets; and all levels of government, including state, local, tribal, and territorial (SLTT) and federal partners.



Annex D: Acronyms

AAR	After-Action Report	MOU	Memorandum of Understanding
BIA	Business Impact Analysis	NARA	National Archives and Records Administration
BPA	Business Process Analysis	NEF	National Essential Function
CAT	Continuity Assessment Tool	NGO	Nongovernmental Organization
CBRNE	Chemical, Biological, Radiological, Nuclear, or Explosive	NIMS	National Incident Management System
CGC	Continuity Guidance Circular	NIST	National Institute of Standards and Technology
CIP	Continuous Improvement Program	PACE	Primary, Alternate, Contingency, Emergency
CISA	Cybersecurity and Infrastructure Security Agency	POC	Point of Contact
COA	Course of Action	POETE	Planning, Organization, Equipment, Training, and Exercises
COG	Continuity of Government	PPD	Presidential Policy Directive
CPG	Comprehensive Preparedness Guide	PSTN	Public Switched Telephone Network
ECG	Enduring Constitutional Government	SLTT	State, Local, Tribal, and Territorial
EMAC	Emergency Management Assistance Compact	SPR	Stakeholder Preparedness Review
EMPG	Emergency Management Performance Grant	THIRA	Threat and Hazard Identification and Risk Assessment
EOP	Emergency Operations Plan	TSP	Telecommunications Service Priority
ESA	Essential Supporting Activity	WMD	Weapons of Mass Destruction
FCI	Federal Continuity Directive	WPS	Wireless Priority Service
FEMA	Federal Emergency Management Agency		
FNARS	FEMA National Radio System		
GETS	Government Emergency Telecommunications Service		
HIPAA	Health Insurance Portability and Accountability Act		
HSEEP	Homeland Security Exercise and Evaluation Program		
HSGP	Homeland Security Grant Program		
IT	Information Technology		
IT/DR	Information Technology/Disaster Recovery		
MEF	Mission Essential Function		
MOA	Memorandum of Agreement		

