









Continuity Guidance Circular

February 2018

FEMA National Continuity Programs

FEMA

Today's threat environment has increased the need for comprehensive continuity plans that enable communities and organizations to continue essential functions and provide critical services across a broad spectrum of emergencies when normal operations are disrupted.

Effective continuity planning is the responsibility of the whole community. Continuity is an important element of preparedness and an integral part of each core capability across the five mission areas of protection, prevention, mitigation, response, and recovery within the National Preparedness System. Because incidents may affect an organization's or government's ability to provide assets, assistance, and services, continuity planning and operations are an inherent component of each core capability and the coordinating structures that provide them. Enduring constitutional government, continuity of government, and continuity of operations is dependent upon the foundation of preparedness built by each and every individual and community. No level of government can perform essential functions and provide critical services without the support of the rest of the Nation. Private sector entities, critical infrastructure, non-governmental organizations, communities, individuals, families, and households play a vital role.

This Continuity Guidance Circular serves as a resource for federal and non-federal entities to guide, update, and maintain organizational continuity planning efforts and appropriately integrate and synchronize continuity efforts. These entities should also engage with partners, stakeholders, and other coordinating structures to integrate organizational continuity plans into community- and government-wide planning efforts.



William B. "Brock" Long
Administrator
Federal Emergency Management Agency

Continuity Guidance Circular Table of Contents

Foreword: A National Continuity Philosophy 1

Introduction 1

Vision and Purpose 3

Continuity Planning 3

Guiding Principles 4

Roles, Responsibilities, and Integration 4

Interface with Other Concepts 6

How to Use this Circular 8

Chapter 1: Getting Started 9

Guidance and Standards 9

Initiating Planning 10

Leadership Support 12

Chapter 2: Building a Capability 14

Step 1: Identify Essential Functions 14

Step 2: Identify Mitigation Options 19

Step 3: Identify Key Elements 21

Step 4: Plan and Implement Options and Elements 26

Chapter 3: Maintaining a Capability 31

Testing, Training, and Exercising 31

Updating and Reviewing Plans and Programs 33

Resource Direction and Investment 34

Multi-Year Strategic Planning 35

Conclusion 36

Appendix 1: Authorities and References 37

Appendix 2: Key Terms 38

Appendix 3: Acronyms 42

Appendix 4: Continuity Planning Checklist 43

Foreword: A National Continuity Philosophy



Introduction

Every day, individuals, organizations, and government institutions provide critical services and conduct essential functions upon which our neighbors and communities depend. These interdependencies are integral to the survival and support of our way of life. Continuity ensures that the whole community has planned for ways to provide essential services and conduct these functions when normal operations are disrupted. Without the planning, provision, and implementation of continuity principles, our organizations, communities, and government may be unable to provide services to help fellow citizens when needed the most. People may die, elected officials may be unable to carry out statutory authorities, organizations may be unable to respond, and communities may be unable to recover.

This Continuity Guidance Circular details the fundamental theories and concepts to unify the application of continuity principles, planning, and programs across the Nation. It provides guidance on the integration of continuity concepts, provides a common foundation for understanding continuity, and guides the development of other tools and resources.

Presidential Policy Directive-21, Critical Infrastructure Security and Resilience, defines resilience as "the ability to prepare for and adapt to changing conditions and recover rapidly from operational disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." Continuity is an important part of ensuring a resilient Nation. It is imperative that federal and non-federal entities strengthen the security and resilience of the United States through systemic preparation for the threats that pose the greatest risk.

The national preparedness and continuity of essential functions for citizens is a shared responsibility across the whole community, building upon a foundation of the resiliency of individuals and local communities and permeating throughout the private and nonprofit sectors, faith-based organizations, and all levels of governments, to include local, regional/metropolitan, state, tribal, territorial, and federal. The importance of the interconnected nature of continuity means that it is not isolated as the responsibility of any sole organization or entity. Continuity is not strictly a governmental responsibility or limited to specific disciplines. Continuity encompasses an interdependent concept and culture that reaches across all communities, organizations, and individuals and should be taken into earnest consideration by all levels of leadership.

A wide range of threats and hazards continue to pose a significant risk to the Nation, affirming the need for an all-hazards, capability-based approach to preparedness planning, to include continuity planning. Comprehensive continuity plans ensure the resiliency of those resources and the means by which they are delivered. Because continuity is an inherent part of preparedness, response operations, and resiliency at all levels, an array of strategies and standards can be employed to ensure the continuation of the core capabilities, essential functions, and critical services from one entity to another. As the Nation continues to evolve and build upon its experiences with each threat and hazard faced, continuity is a driving force to ensure that everyone is able to provide for and receive essential functions and services.

Why Continuity?

Regular Day

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



Continuity Event

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



Vision and Purpose

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. The concept of continuity and a resilient Nation can never be a one-size-fits-all program, but one that evolves to suit the environment faced.

To support a unified continuity doctrine, the objectives of this Circular are to:

- Describe, across the whole community, the relationships involved to establish and maintain a comprehensive and effective continuity program to ensure resilience, the continuing performance 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 and coordination of continuity activities.
- Outline continuity guiding principles to inform planning, coordination, and operations.
- Describe scalable, flexible, and adaptable coordinating structures, as well as key roles and responsibilities for integrating continuity plans across the whole community to support national resilience and essential functions.

This Circular serves as a resource for federal and non-federal entities to appropriately integrate and synchronize continuity efforts. Non-federal entities, to include non-governmental organizations, private sector entities, local governments, schools and academia, and state, tribal, and territorial governments can draw upon this Circular as a reference when creating or revising continuity plans, programs, and processes.

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.

Continuity Planning

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.

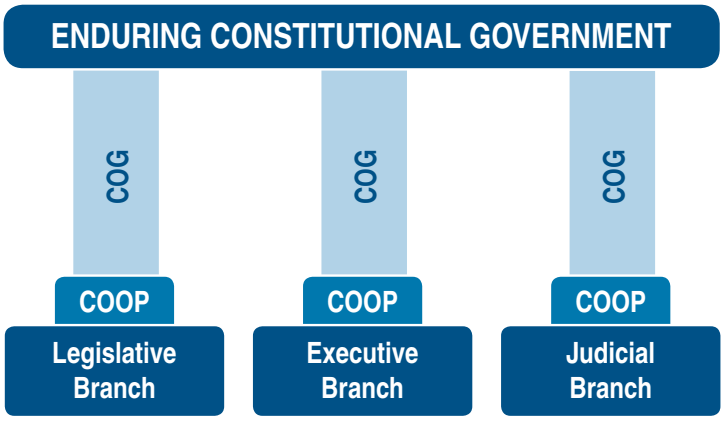
Continuity of operations (COOP) ensures an individual organization can continue to perform its essential functions, provide essential services, and deliver core capabilities during a disruption to normal operations. Effective continuity of operations activities provide a baseline capability and represent the minimum standard required by a comprehensive, integrated national continuity program.

Continuity of government (COG) is a coordinated effort within each of the executive, legislative, and judicial branches to ensure that essential functions continue to be performed before, during, and after an emergency or threat. COG is an outcome of a viable continuity capability, not a program. Continuity of government is intended to preserve the statutory and constitutional authority of elected officials at all levels of government across the United States.

Disasters can cause local or regional COG scenarios by threatening the ability of jurisdictions to execute their statutory authorities, perform essential functions, and deliver essential services. COG should be scalable and flexible to meet the requirements, threats, and needs of the supported organizations or jurisdictions, whether small localities, large cities, or state, territorial, or tribal governments.

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. 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 support essential functions during an emergency. Jurisdictions may not delineate separate planning efforts for COG and ECG, especially among smaller communities. However, the goal of ensuring a functioning government for its citizens remains the same.

Continuity of operations ensures that individuals can perform an organization's essential functions. Continuity of government ensures the integrated, collective performance of essential functions by a branch of government. Enduring constitutional government safeguards the functionality all three branches of government—executive, legislative, judicial—at any level. Continuity enhances the resilience of organizations, the whole community, and, in turn, the Nation by ensuring the preservation of government structures.



Guiding Principles

The potential for no-notice emergencies, including localized natural hazards, accidents, technological emergencies, and terrorist attacks, require 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

A prepared and resilient Nation is built upon 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 of protection, prevention, mitigation, response, and recovery within the National Preparedness System. The National Preparedness Goal identifies core capabilities, which are activities that address the greatest risks to the Nation. Continuity is an important element of preparedness and an integral part of each core capability across the five mission areas of protection, prevention, mitigation, response, and recovery within the National Preparedness System. The National Preparedness Goal identifies core capabilities, which are activities that address the greatest risks to the Nation. Continuity planning and operations increases the likelihood that organizations can perform essential functions and deliver core capabilities and essential services. Because incidents may affect an organization's ability to provide assets, assistance, and services, continuity planning and operations are an inherent component of each core capability and the coordinating structures that provide them.

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 cannot be strong if the communities that comprise it are vulnerable to the effects of the threats and hazards that it faces. 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 nongovernmental organizations and the general public, in conjunction with the participation of all levels of government in order to foster better coordination and working relationships." The National Response Framework lists whole community contributors as "children; older adults; individuals with disabilities and others with access and functional needs; those from religious, racial, and ethnically diverse backgrounds; people with limited English proficiency; and owners of animals, including household pets and service animals." Every community and organization, no matter how large or how small, has essential functions that support the continuation and resiliency of the Nation. No one entity, including the federal government, can perform all of the functions and services without the support of the rest of the Nation. Multidiscipline and multijurisdictional partnerships are critical in developing and sustaining an effective continuity capability.

3. Scalable, Flexible, and Adaptable Continuity Capabilities

No organization or entity is the same; they vary in size and complexity. This Continuity Guidance Circular takes this diversity into consideration. A comprehensive continuity program and culture requires continuity programs and capabilities to be scalable, flexible, and adaptable to meet evolving requirements. As needs grow and change, continuity must remain nimble and adjustable in order to achieve the vision set forth in this document.

Roles, Responsibilities, and Integration

This Continuity Guidance Circular is intended to be used by the whole community. This 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. All elements of the community must be activated, engaged, and integrated in order to continue essential functions during any incident that may disrupt operations.

The most effective partnerships within a community capitalize on multidisciplinary coalitions and all available resources—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 prior to and during incidents reduce disruptions to essential functions and critical services. There are a multitude of existing coordinating structures in which continuity planners should participate to integrate continuity planning, operations, and responsibilities into emergency management, preparedness, and resilience efforts.

FEMA's Comprehensive Preparedness Guide 101, *Developing and Maintaining Emergency Operations Plans*, outlines the importance of engaging in community-based planning—planning that is for the whole community and involves the whole community. Continuity-specific roles of whole community members include:

- **Individuals, Families, and Households:** Individuals, families, and households play an important role by executing essential functions and providing critical services, so impacts to the people jeopardizes the continued performance of essential functions.
- **Communities:** Engaging community groups and promoting a culture of continuity, while 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.
- **Non-Governmental Organizations (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 write their own continuity plan 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 for the rapid reestablishment of normal commercial activities and critical infrastructure operations following a disruption. Since most critical infrastructure resides within the private sector, collaborating with these coordination structures is a key element of ensuring the continuity of essential functions and critical services. The private sector will also play a key role in reconstituting organizations and governments. These organizations are critical to the Nation being able to continue to perform essential functions and provide critical services.
- **Local Governments:** Because they work to protect the health, safety, and welfare of the people they represent, local governments bear responsibility for continuity planning and operations. It is incumbent upon local governments to best apply a localized understanding of risks and hazards in order to most effectively plan and implement continuity strategies and programs. Local governments are directly connected to community plans and are the providers of critical services and essential functions to its citizens. State, tribal, and territorial governments and the federal government relies upon local governments to be able to ensure that the local communities are able to perform their essential functions. Ultimately, the essential functions of all levels of government contribute directly to national resilience, continuity of government, and enduring constitutional government.

- **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 operations efforts.
- **Tribal Governments:** As sovereign nations, tribal governments govern and manage the safety and security of their lands and community members. 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 continuity, the federal government cannot sustain and perform its essential functions without the support and integration of efforts of federal and non-federal entities. Most federal departments and agencies have regional or field offices that may participate with state and local governments in continuity planning through working groups and integrated test, training, and exercise events. At the Headquarters level, Continuity Coordinators at the Assistant Secretary-level attend the Continuity Advisory Group, which is a continuity policy coordination group that provides a forum to identify interagency continuity challenges; obtain continuity-related information; and collaborate on continuity planning.
  - **Federal Emergency Management Agency (FEMA):** Presidential Policy Directive-40, *National Continuity Policy*, designates FEMA to, among other tasks: "coordinate the implementation, execution, and assessment of continuity operations and activities among executive departments and agencies; develop and promulgate Federal Continuity Directives to establish continuity program and planning requirements for executive departments and agencies; develop, lead, and conduct a federal continuity training and exercise program; develop and promulgate continuity planning guidance to state, local, territorial, and tribal government, nongovernmental organizations, 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; and 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."

Vermont's Response to Tropical Storm Irene

Lessons Learned from a Continuity Planning Perspective

On August 28, 2011, the state of Vermont experienced the largest natural disaster since the Great Flood of 1927 – Tropical Storm (TS) Irene. The damage from TS Irene caused the displacement of approximately 1,500 state employees, and flooding and widespread power outages rendered several permanent primary worksites unusable, including the State Emergency Operations Center (EOC). State agencies activated continuity plans to sustain the performance of essential functions, including using alternate locations and relocating the State EOC.

One of several strengths identified during TS Irene was that each state agency maintained a continuity plan. However, several continuity plan assumptions conflicted with actions associated with the long-term displacement from primary facilities. This impacted the execution of some essential functions. For example, one agency's alternate site was the primary site for another agency.

Through a thorough analysis of the operations of state, regional, and local entities, the state of Vermont developed an impressive plan to address improvements in continuity planning. The improvement plan de-conflicted planning assumptions and addressed the need for regular exercising of continuity plans at all levels.

(Note: Our thanks to the State of Vermont for providing the data used in this case study.)

Interface with other Concepts

The ability to continue the performance of essential functions and provide critical services is greatly enhanced with the right people, resources, and planning. Continuity of these capabilities 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 assists communities in working 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. Proper testing, training, and exercising among the whole community helps delineate roles and responsibilities and deconflict procedural, resource, and personnel issues.

- **Incident Command System:** Organizations should integrate continuity planning with incident management planning and operations, to include responsibilities outlined in the National Response Framework. 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/Facility Emergency Plans:** Occupant emergency programs and plans and facility emergency plans establish basic procedures for safeguarding lives and property in and around a facility during emergencies. It describes the actions occupants should take to ensure their safety in an emergency situation. 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 need to account for such situations and plan accordingly to ensure essential functions and critical services 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 when needed when normal operations are impacted or necessary resources are unavailable. FEMA's Comprehensive Preparedness Guide 101, *Developing and Maintaining Emergency Operations Plans,* is designed to help both novice and experienced planners navigate the EOP planning process. Used in its entirety, the Guide provides information and instruction on the fundamentals of planning and its application.
- **Information Technology/Disaster Recovery (IT/DR) Plans:** It is a common misconception that IT/DR plans are synonymous with or a substitute for a continuity plan. IT/DR plans complement continuity plans, and the two plans should be coordinated. An IT/DR plan does not account for how an organization will continue its

essential functions during an emergency. However, the IT/DR plan impacts an organization's continuity plans and operations by identifying recovery time objectives for key systems that support the performance of functions, including essential functions.

- **Pandemic Plans:** A pandemic or infectious disease plan is a strategy for organizations to mitigate illness, suffering, and death of its staff while sustaining the ability to provide services and perform essential functions through a period with significant employee absenteeism. Because a pandemic or other infectious disease spread may trigger a continuity plan activation, such plans have an important role in an organization's overall continuity plan and should be coordinated. Aspects of an organization's pandemic and infectious disease Plan may be used in non-pandemic incidents that may impact the ability of personnel to report to work.
- **Business Continuity Plans:** Business continuity plans are similar to continuity plans in that the plans enable the continued functioning of businesses following an incident. Business continuity plans also address key variables that allow business to minimize lost revenues and maximize profits. When businesses are disrupted, insurance may not cover all costs and cannot replace customers that defect to competitors. However, these businesses may have a direct role in ensuring the resiliency of the communities in which they reside. The information contained within this Continuity Guidance 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 resiliency through the execution of robust and integrated continuity plans.

How to Use this Circular

This Continuity Guidance Circular is designed to present the overarching guiding principles behind the incorporation of continuity planning throughout the whole community. Tasks and functions performed by an individual flow upward to support his or her community, whether it's through his or her job or volunteering. Public and private sector entities, staffed by those individuals, support the provision of critical services and essential functions. Enduring constitutional government, continuity of government, and continuity of operations is dependent upon the foundations of resilience and preparedness built by each and every individual and community in the face of threats and hazards. Every level of government, every sector of critical infrastructure, and every public and private organization has a role to play and must interface and integrate with each other in order to build and maintain a resilient Nation.

These entities and organizations can use this Continuity Guidance Circular to guide, update, and maintain organizational continuity planning efforts. These entities should also engage with partners, stakeholders, and other coordinating structures to integrate organizational continuity plans into community- and government-wide continuity plans. This Continuity Guidance Circular does not make current continuity plans and programs obsolete. However, to promote consistency across the Nation, entities are encouraged to review the Circular 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 within this Circular. This Continuity Guidance Circular supersedes Continuity Guidance Circular-1, *Continuity Guidance for Non-Federal Governments,* dated July 2013 and Continuity Guidance Circular-2, *Continuity Guidance for Non-Federal Governments: Mission Essential Function Identification Process,* dated October 2013.

FEMA has developed a supporting Continuity Resource Toolkit that provides examples, tools, and templates for implementing each chapter of this Circular. In the future, FEMA will continue to build and distribute tools and information to assist federal and non-federal entities develop and maintain a successful continuity program and plan.

The Toolkit is found at: www.fema.gov/continuity-resource-toolkit.

Continuity Planning Checklist

- ☐ Examine current state of 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 in to integrate continuity planning, operations, and responsibilities into emergency management, preparedness, and resilience efforts.
- ☐ Identify other inter- and intra-organizational continuity plans and programs (e.g., incident management, Occupant Emergency Plans, and Emergency Operations Plans, IT/Disaster Recovery Plans), which should be coordinated with to ensure synchronization across plans and programs.

Chapter 1: Getting Started

Continuity planning is simply the good business practice of ensuring the execution of essential functions and provision of critical services and core capabilities through all circumstances. Today's threat environment and the potential for no-notice emergencies, including localized natural hazards, accidents, technological emergencies, and terrorist attack-related incidents, underscore the need for strong continuity planning that enables all communities, organizations, and entities to continue essential functions across a broad spectrum of emergencies.

Before initiating the development of or update to plans and procedures, an organization should create an overall continuity strategy that is agreed upon by elected officials or organizational leadership. This chapter identifies foundational elements of a continuity program that will increase the success of continuity planning and operations. Planners and managers responsible for continuity should consider, implement, and enhance these elements to ensure the success of their organization.



Guidance and Standards

Numerous public and private sector standards, laws, codes, and guidance exist to guide continuity planning and operations and its integration with preparedness, emergency management, mitigation, and recovery. Under the *National Continuity Policy*, FEMA has the responsibility to develop and promulgate continuity program and planning requirements for federal executive branch departments and agencies and develop and promulgate continuity planning guidance to state, local, territorial, and tribal government, nongovernmental organizations, and private sector critical infrastructure owners and operators. Federal executive branch departments and agencies are governed by the requirements outlined in the *National Continuity Policy* and Federal Continuity Directives 1 and 2. Many states have a gubernatorial mandate requiring state agencies develop continuity plans. Numerous counties, municipalities, and other government organizations require continuity programs. Public and private sectors, such as healthcare and banking, have 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 Continuity Guidance Circular outlines a continuity planning framework with principles and tools that an organization can adopt. The decision of what continuity strategies and requirements to use is dependent

on many considerations, including resources, size, and organizational functions. Ultimately, implementation of and adherence to a continuity standard or 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 its citizens depend. Establishment or adoption of a standard enables a coordinated planning process and establishes a policy-level framework to guide decisions made during continuity planning and implementation. Development and adherence to a community- or state-level policy enables operational coordination, as the activation of a continuity plan may also entail the activation of cross-organizational support agreements.

Initiating Planning

When initiating continuity planning, organizations are encouraged to:

- **Become knowledgeable with the current program** by reading existing plans and procedures. If a continuity plan or procedures do not exist, planners should determine if other emergency plans that interface with continuity, like Occupant Emergency Plans and pandemic plans, exist.
- **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 upon size, mission, and resources, organizations and jurisdictions may choose to combine responsibilities under one or more of these roles. Common titles, roles, and responsibilities include:
  - **Leadership and elected officials.** The requirements and responsibilities of leadership and elected officials is discussed in more detail in the next section. Leadership and elected officials are ultimately responsible for ensuring the organizations for which they are responsible can continue the performance of essential functions and delivery of critical services when normal operations are disrupted.
  - **Continuity Coordinator.** The 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 manager and other continuity planners within subcomponent levels throughout the organization or government.
  - **Continuity Manager.** The senior continuity planner responsible for coordinating overall continuity activities within the organization or jurisdiction. This individual managing day-to-day continuity programs, coordinating continuity planners within the organization, representing his/her organization's program externally, as appropriate, and reporting to the Continuity Coordinator on continuity program activities.
  - **Continuity Planner.** The continuity planner 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.

Colorado Department of Transportation

Leveraging Daily Operations to Enhance Continuity Planning

Leveraging and coordinating ongoing efforts within the organization can enhance continuity planning efforts to enable a successful program. The Colorado Department of Transportation is using an upcoming facility move to update its continuity plan and program, exemplifying how a state agency has integrated continuity concepts into daily operations.
In spring 2018, the Department of Transportation will consolidate two buildings into a new primary facility, a move that will affect approximately 800 staff and 23 programs. Planners are directly leveraging efforts related to the move to enhance the Department's continuity program and plan.

The Department is digitizing records, storing the records on the cloud, and upgrading the virtual private network (VPN). These efforts enable access to the records from any location, including from alternate locations and telework sites. Staff in each program office are working with the Records Management Office to review and update files, identify those records used on a daily basis, and archive documents no longer needed.

As a state agency, the Department of Transportation has staff that work throughout the state; the agency is using the upcoming move as an opportunity to update contact and call down lists. This directly benefits the continuity program by enabling contact and communication with all staff in the event of a continuity activation.

State agencies in Colorado are required to update continuity plans on an annual basis. The Colorado Department of Transportation will be using lessons learned from the office move to update and enhance its continuity plan during its next annual update. The office move will also drive the Department to update its continuity plan based upon the new location, which may impact risks to essential functions, mitigation strategies to reduce those risks, and other continuity processes and procedures.

(Note: Our thanks to the Colorado Department of Transportation for providing the data used in this case study.)

- **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 assists the continuity program and planning effort. This team is described in more detail in the next bullet.
- **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.

To assist continuity coordinators, planners and managers in developing and maintaining continuity plans and programs, FEMA has established a continuity training program that addresses the full spectrum of continuity planning. Through training events, personnel can develop and enhance their continuity knowledge and expertise. Courses are available for students at all levels, from individuals new to continuity planning to program managers who have been involved with continuity for many years. FEMA established the Continuity Excellence Series - Level I, Professional Continuity Practitioner, and Level II, Master Continuity Practitioner, certificate program to enhance the excellence in the development and implementation of Continuity programs and emergency management. For additional details, please visit the Continuity Resource Toolkit at www.fema.gov/continuity-resource-toolkit.

- **Establish a continuity planning team to assist with planning,** as one person alone cannot develop the continuity plan. Once a continuity plan is developed, this team can continue to meet periodically to maintain the continuity program, including updating the plan and develop training and exercises. Examples of others needed to assist include representatives from:
  - **Each organizational office.** These offices conduct an organization's functions and services on a daily basis and are needed to provide details and expertise to the Business Process Analysis and planning effort and staff and support essential functions and critical services during a continuity activation;
  - **Information Technology.** Technology, including communications, critical systems, and data, is the foundation of many tasks, activities, functions, and capabilities. Experts play a key role ensuring these resources are available in a continuity activation. See Section 3.2 for additional details;
  - **Human Resources.** Organizations should facilitate dialogue among human resources and continuity planners when developing continuity plans and programs. Topics to address include incorporating commonly requested reasonable accommodations into the plan and designating employees as continuity personnel, telework-capable to support continuity operations, and excused from duty due to the emergency situation;
  - **Facilities Management.** Facility managers 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 facility and planning for reconstitution;
  - **Comptroller.** Organizations must align and allocate the resources needed to implement its continuity strategy. Through the budgeting and planning process, an organization's leaders and staff ensures the availability of critical continuity resources needed to continue the performance of the organization's essential functions before, during, and after an emergency or disruption;
  - **Security.** Security strategies are needed that address personnel, physical, and information security to protect plans, personnel, facilities, and capabilities and to prevent adversaries from disrupting continuity plans and operations;
  - **Legal.** An organization's legal department or equivalent should develop and review the delegations of authority, orders of succession, and Memorandums of Agreement/Memorandums of Understanding to ensure legal sufficiency; and
  - **Bargaining unit or union representation, if applicable.** Organizations should work with bargaining units and labor unions in developing and bargaining over such procedures where bargaining unit employees were impacted.
- **Develop a project plan, timelines, and milestones.** Identifying a project plan, timelines, and milestones will assist the team in determining if the planning effort is efficient and effective.
- **Identify preliminary budgeting and resource requirements.** An organization will develop a detailed budget during the continuity planning process, once essential functions, mitigation strategies, and resource requirements are identified. However, the team should identify an initial budget estimate during this phase, particularly for expected costs and resources needed to develop the continuity plan and program.

Leadership Support



Because continuity extends through the entire Nation, from the national government to local communities and across all levels of organizations, it is imperative that its importance is recognized by elected officials and leadership. Leadership must articulate a commitment to continuity in order for a culture of continuity readiness and preparedness to permeate throughout the organization, community, and government. In addition to promoting a culture of preparedness within individual organizations, leadership and elected officials are necessary to oversee a comprehensive planning environment by coordinating and integrating continuity and emergency plans with interdependent stakeholders internal and external to the organization in order to build a resilient community and Nation.

Leadership and elected officials are held directly responsible when citizens do not receive the essential services on which they depend or when an organization cannot continue its essential functions in an emergency. Leadership is also directly responsible for ensuring that continuity plans and programs are successfully developed, coordinated, exercised, and implemented. Effective implementation of continuity plans and programs requires the support of leadership and decision makers who have the authority to commit the organization and the necessary resources to support continuity programs. Continuity preparedness encompasses more than information technology (IT) or facilities; it is the continuation of the functions, capabilities, and services that the organization provides to its stakeholders.

Obtaining leadership and elected official support of continuity planning and preparedness can be difficult when faced with shrinking budgets, competing priorities, and additional duties. Continuity can be seen as an "insurance policy," and funding, personnel, and support is diverted to needs perceived as more urgent. As a continuity planner or manager, several options and tools are available to assist in obtaining the support of leadership and elected officials for the continuity program.

1. **Identify preparedness or emergency management forums or working groups** in which your senior leaders 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. Forums also allow for highlighting best practices, lessons learned, and interdependencies from your organization and others.

2. **Conduct test, training, and exercise events.** Pre-exercise planning and exercise play may illuminate shortcomings and highlight the need for additional support or resources.

3. Relate continuity to your organization's mission and priorities. Leadership is already focused on and understands the mission and priorities of its organization. Linking continuity to these can enhance the support and focus on the continuity program.

4. **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. Including continuity planning milestones and continuity metrics within a leader's performance plan or evaluations helps ensure a continual focus and commitment to the continuity program.

5. **Find a continuity champion.** In many organizations, there is an individual who supports continuity and views it as a priority. However, this individual may not be the head of the organization or an immediate supervisor. Including these individuals in the planning process allows them to advocate to others on behalf of the continuity program.

FEMA has developed a supporting Continuity Resource Toolkit that provides examples, tools, and templates for implementing each chapter of this Circular. In the future, FEMA will continue to build and distribute tools and information to assist federal and non-federal entities develop and maintain a successful continuity program and plan.

The Toolkit is found at: www.fema.gov/continuity-resource-toolkit.

Continuity Planning Checklist

- ☐ Create an overall continuity strategy that is agreed upon by elected officials or organizational leadership.
- ☐ Identify existing, applicable continuity regulations or requirements. In the absence of requirements, identify continuity guidance, and principles most applicable to the organization.
- ☐ Identify continuity program planning roles and responsibilities.
- ☐ 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.
- ☐ Obtain the support of leadership and elected officials for the continuity program.

Chapter 2: Building a Capability

Continuity responsibility and planning should not be a separate and compartmentalized function performed by independent cells of a few planners in each organization. Organizations must fully integrate continuity into all aspects of their daily operations, creating a culture of continuity. This chapter aims to provide guidance and a framework for building a comprehensive continuity foundation and plan that is coordinated with partners and stakeholders.



Step 1: Identify Essential Functions

The National Essential Functions (NEFs) are the foundation of all continuity programs and capabilities and are the primary focus of the federal government before, during, and after a catastrophic emergency. However, the federal government cannot maintain these functions and services without the support of the rest of the Nation; the whole community directly contributes to the federal government's ability to perform the NEFs. The NEFs are accomplished through a collaborative effort with federal departments and agencies performing various essential functions, integrated and supported by states, territories, tribes, local governments, the private sector, non-governmental organizations, and the public.

The National Essential Functions (NEFs)

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.*
2. *Provide leadership visible to the Nation and the world and maintain the trust and confidence of the American people.*
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.*
4. *Maintain and foster effective relationships with foreign nations.*
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.*
6. *Provide rapid and effective response to and recovery from the domestic consequences of an attack or other incident.*
7. *Protect and stabilize the Nation's economy and ensure public confidence in its financial systems.*
8. *Provide for federal government services that address the national health, safety, and welfare needs of the United States.*

Non-federal entities should identify its own essential functions that align to the NEFs. Component or government agencies identify essential functions and critical services necessary to accomplish this overarching mission. Other agencies, organizations, and entities, both public and private sectors, may also find that their functions are nested within these higher level essential functions and play a direct role in insuring the continuation of governmental functions. Examples of how non-federal essential functions align to the NEFs include:

1. **Maintain continuity of government,** focusing on the continued functioning of critical government leadership elements, including: succession to key offices, such as those of the Governor, mayor, or parish, local, or county executive; communications within the branches of government, government agencies, and the public; leadership and management operations; situational awareness; and personnel accountability. This falls under the umbrella of NEF 1.

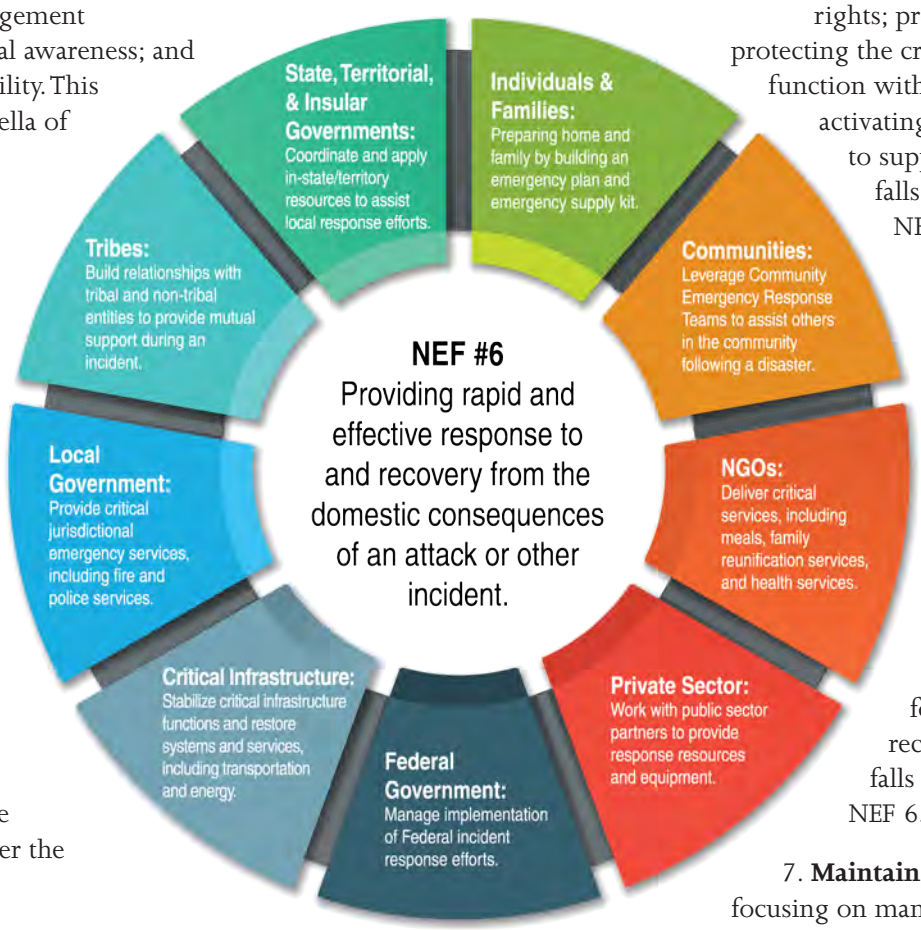
2. **Provide visible leadership,** focusing on visible demonstration of leaders effectively dealing with crisis and leading response efforts. Essential functions can include monitoring threats and hazards and maintaining the confidence of established government organizations and the public. This falls under the scope of NEF 2.

3. **Support the defense of the United States.** While the primary responsibility for defending the Nation lies within the federal government, other organizations and individuals support NEF 3. Individuals comprise the military, and these individuals are supported by numerous organizations and volunteer agencies. Critical infrastructure and the private sector also play a key role.

4. **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 tribes. This includes communications and interactions, as necessary, during a crisis with critical partners and organizations, including the federal government; other state, territorial, tribal, and local governments; private sector and non-profit 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.

5. **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 the critical infrastructure. A function within this area includes activating National Guard units to support these efforts. This falls under the scope of NEF 5.

Example Whole Community Essential Functions in Support of a NEF



6. **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. This falls under the umbrella of NEF 6.

7. **Maintain economic stability,** focusing on managing the overall economy of the locality. While the federal government is responsible for protecting and stabilizing the national economy and regulating the currency, non-federal governments have a responsibility to manage their jurisdiction's finances, ensure solvency, and ensure banks, credit unions, savings and loans, and stock and commodity exchanges can open and transact business in accordance with legal obligations, to include any

power and data services required for transactions. During a crisis affecting the economy, maintaining confidence in economic and financial institutions is critical at every level of the government. This falls under NEF 7.

8. **Provide basic essential services,** focusing on providing water, power, healthcare, including disability support services and personal assistance services, communications, transportation services, sanitation services, environmental protection, commerce, education, and child care. 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 a return to normalcy. This falls under the scope of NEF 8.

Whole community engagement, one of the guiding principles of continuity planning, is required for governmental essential functions to be able to continue throughout all hazards. No level of government can perform essential functions and provide critical services without the support of the rest of the Nation. Private sector entities, critical infrastructure, non-governmental organizations, communities, individuals, families, and households play a vital role in support of essential functions. Each person and organization is a crucial link in a chain of tasks and activities that enable the performance of essential functions. Multidiscipline and multijurisdictional partnerships are critical in developing and sustaining a culture of continuity that is meaningful, effective, and provides a foundation for the safety, security, and the continuation of government upon which the Nation is built. Without individuals doing their jobs or tasks, without infrastructure enabling the personnel and resources to have the tools necessary to do their jobs, without the businesses that provide those resources, and without the communities providing services to their citizens, the Nation cannot sustain itself in the threats and hazards that it faces.

1.1 Conduct a Risk Assessment

Risk management is 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. Effective risk management practices and procedures assist organizations in accomplishing continuity objectives. A risk management program includes continuity of operations as part of its risk mitigation strategy.

There are many different 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 analysis of critical infrastructure interdependencies. These risk assessments inform the Business Impact Analysis (BIA) process. Risk assessments that entities can leverage include the Hazard Mitigation Plan's Hazard Identification and Risk Assessment, local facility-based Hazard Vulnerability Analyses, cyber and information security assessments, or other risk assessments available at the community or regional level. 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 tribes use the THIRA process to consider relevant threats and hazards, give them context, and identify their potential impacts. Jurisdictions 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 Comprehensive Preparedness Guide 201, *Threat and Hazard Identification and Risk Assessment Guide,* outlines the process for conducting a Threat and Hazard Identification and Risk Assessment.

Many methods of conducting risk assessments exist, but a risk assessment, should answer the following questions:

1. What are the threats and hazards that the organization faces?
2. What are the characteristics of the threats and hazards (how may the threat and hazard affect the organization)?
3. What is the likelihood of occurrence for the threat or hazard?
4. What would be the overall risk value for the threat or hazard?

1.2 Conduct a Business Process Analysis

An important first step in creating a continuity program is to identify the essential functions of an organization and its relationships to NEFs and other essential functions. In order to do so, an entity must conduct a Business Process Analysis (BPA).

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 facilities inherent in the execution of a function or requirement. An effectively conducted BPA supports the development of detailed procedures that outlines how an organization accomplishes its mission.



Each organization should look at the BPA process from the point of view of both the big picture (the overall process flow and 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 will result in developing guidelines for performing essential functions that fall under the umbrella of a NEF or an organization's essential functions.

A detailed BPA identifies and answers:

1. What products, information, and equipment are required for this task, from both internal and external partners?
2. What products, services, and information result from the performance of this task (including metrics that identify specific performance measures and standards)?
3. Who in the organization's leadership is required to perform the task, if direct leadership involvement is needed?
4. What staff internal or external to the organization is required to directly support or perform the task (including specific skill sets, expertise, and authorities needed)?
5. What communications and IT software and equipment are required to support the task (including any unique or unusual requirements)?
6. What are the facility requirements for performing the task (e.g., facility type, square footage, security, infrastructure required)?
7. What supplies, services, capabilities (not already addressed) are required to perform the task (including the ability to obtain, purchase, and relocate these resources)? What are the funding sources?
8. Who are the internal and external organizations that support or ensure task performance and what information, supplies, equipment, or products do they provide?
9. From start to finish, how is the task performed?

1.3 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 (gaps, weaknesses, 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 or crisis occurs, an organization can perform its essential functions. The results of the BIA will establish the foundation of evaluating and establishing risk mitigation strategies to ensure the continued performance of organizational essential functions and delivery of critical services.

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

1. What is the vulnerability of the essential function to each threat or hazard identified in the risk assessments?
2. What would be the impact if the essential function's performance is disrupted?
3. What is the timeframe for unacceptable loss of functions and critical assets?

When executing a risk management process for continuity operations, organizations should consider a range of factors, such as the probabilities of events occurring, mission priorities, legal requirements, and impact assessments. Organizations should also consider cost because informed decisions about acceptable and unacceptable levels of risk will ultimately drive the expenditure of resources, including money, people, and time, to mitigate risk. Organizations can never eliminate risk, because no organization can afford to counter every threat to its mission. Successful continuity planning demands an intelligent analysis and prioritization of where and when to focus resources, funding, and other assets. Risk management requires leadership and staff to think beyond the internal effects of the organization's inability to perform its essential functions. Organization leaders and staff at all levels need to also consider the interdependencies between and among organizations that share critical roles in the delivery of capabilities. Because of the synergistic relationship between organizations, organizations need to coordinate planning between all levels and branches of government and the private and public sectors.

Some essential functions are focused on the continued provision of services that stakeholders, partners, and customers expect to be provided on a regular and

uninterrupted basis. Other essential functions are focused towards the direct response to and recovery from an emergency, incident, or disaster. In both cases, conducting a well-organized and methodical BIA process, informed by risk assessments, to create the understanding of what could happen, what the effects of an incident could be, and how to lessen those effects is a key principle of continuity planning.

1.4 Identify and Prioritize Essential Functions

Essential functions are activities and tasks that cannot be deferred during an emergency; these activities must be performed continuously or resumed quickly following a disruption. A distinction should be made between essential and important functions. There are many important functions that can be deferred until after a crisis. Examples of important functions that can be deferred include training and research and development. Just because some functions are not identified as essential does not mean that those functions are considered unimportant. This is sometimes a difficult distinction to make. In many cases, legally mandated functions will be essential, as are functions that are critical to supporting another organization's essential functions. This is where a comprehensive BPA and BIA will help guide an organization in identifying essential functions.

Once a BPA and BIA is conducted, an organization can identify and prioritize their functions to determine which ones should be considered essential functions and in what priority.

Not all of the tasks and activities identified during the BPA can be done in a resource scarce environment. The distinction between essential and non-essential functions is whether or not an organization must perform a function during crisis. Essential functions are those that have to continue during emergencies. Essential functions are both important and urgent. If an organization determines that a function may have to continue during or immediately after an emergency, that organization will identify it as essential.

While not all identified tasks and activities can be performed in the austere environment of an emergency, certain functions cannot be discarded. Legally required activities, like maintaining protections of certain classes of people—race, color, religion, national origin, age, sex, and disability—is essential. For example, an emergency does not abdicate an organization's responsibility to ensure 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.

While performance of all functions will eventually need to resume following a disruption, if resources are limited, an organization may have to prioritize some functions before others. Some functions may require continuous performance while the resumption of other functions may be delayed for short periods of time. But even with essential functions, it may be possible to delay resumption for several days. Organizations should elevate the priority of essential functions that directly support the NEFs.

In addition to the NEFs, continuity planning requirements for the federal executive branch delineates additional categories of essential functions to assist with prioritization. Mission Essential Functions (MEFs) are the essential functions directly related to accomplishing the organization's mission as set forth in statutory or executive charter. Generally, MEFs are unique to each organization. Primary Mission Essential Functions (PMEFs) are those mission essential functions that must be continuously performed to support or implement the uninterrupted performance of NEFs. Essential supporting activities (ESAs) are functions that support performance of MEFs but do not reach the threshold of MEFs or PMEFs. ESAs are important facilitating activities performed by most organizations (e.g., providing a secure workplace, ensuring computer systems are operating); however, the sole performance of ESAs does not directly accomplish an organization's mission.

Several factors must be included in the essential functions prioritization determination, including the following:

1. **Recovery Time Objective:** How quickly must this task or activity resume if disrupted?
2. **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? Does this function have an impact to a NEF?
3. **Management Priority:** What is your organizational leadership's preference and discretion?

Categorizing functions assists organizations with the prioritization of limited resources during an emergency in order to best support their communities during and after an incident. Priorities can be fluid and situation-dependent. For example, plowing snow off 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 attempting 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 Federal Continuity Directives 1 and 2.

Step 2: Identify Mitigation Options



Identifying mitigation options to address risks allows organizations to manage those risks with relevant, comparable, and scoped options. Decision makers need to be able to consider the feasibility of implementing options to support continuity and how various alternatives affect and reduce risk. This includes the consideration of resources, capabilities, time to implement, political will, legal issues, potential impact on stakeholders, and the potential for unintentionally transferring risk within the organization. In terms of continuity, there are several options that can be considered to help mitigate the impact of a disruption on essential functions. This section outlines several mitigation options that organizations can consider.

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. Implementing physical mitigation strategies and reducing long-term vulnerabilities, combined with continuity of operations and recovery planning before a disaster, increases resiliency and the likelihood that communities and organizations can perform essential functions and deliver core capabilities after an incident. Physical mitigation strategies that could increase the resilience of an organization and reduce disruption to essential functions include:

1. Implementing structural changes, such as elevating facilities, flood proofing, or implementing earthquake retrofitting measures;
2. Hardening infrastructure, including implementing security measures for facilities, systems, and applications or re-rerouting utilities underground;
3. Creating redundancy, such as using dual power feeds or uninterruptable power supply; and
4. Geographical dispersion of an organization's normal daily operations.

2.1 Alternate Locations

Alternate locations are sites where organizations can continue or resume essential functions that are not the primary operating facility and where organizational command and control of essential functions occurs during a catastrophic emergency. An Alternate location should be at a sufficient distance from the primary operating facility, not susceptible to the risks associated with the primary operating facility, and accessible to individuals with disabilities. When identifying and preparing alternate locations, organizations should maximize the use of existing local or field infrastructures, including the use of joint or shared facilities. During the planning stage, organizations should identify alternate locations that are accessible to individuals with disabilities. If none are available, organizations should work with facility managers to develop steady-state modifications to the site to ensure readiness during an emergency.

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, other information technology 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 information technology, and environmental infrastructure which is capable of providing backup after additional personnel, equipment, supplies, software, or customization is 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 it can be used.

Organizations should consider using existing organization or other space for alternate locations, such as:

1. **Remote/offsite training facilities:** These facilities may include an organization's training facility located near the organization's primary operating facility, but far enough away to afford some geographical dispersion.
2. **Space procured and maintained by another organization:** Some organizations offer space procurement services that other organizations can use for alternate locations.
3. **Participation in joint-use alternate locations:** Several organizations may pool their resources to acquire space they can use jointly as an alternate location. 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 operating facility, but each organization should have individually designated space and other resources at that location to meet its own needs.
4. **Alternate use of existing facilities:** In certain types of continuity plan activations, organizations may use a combination of facilities and strategies, 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.

The use of alternate locations may not work for all organizations and the effectiveness of this option will be dependent upon factors identified during the BPA, including resource requirements and flexibilities.

2.2 Telework

There is a direct relationship between an organization's continuity plan and telework. The two programs share the basic objective of performing and maintaining an organization's functions in an alternative location and method. Telework can assist the sustainment of essential functions during a change in normal operating status, such as a pandemic or an incident that causes a building closure. In recognition of the value telework can add to continuity capabilities, the Telework Enhancement Act was signed into law in 2010, requiring federal executive agencies to incorporate telework into continuity plans.

When using telework as an option to support essential functions during a continuity plan activation, 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 must 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 at telework locations. Organizations should also coordinate with their IT specialists to identify equipment and technical support requirements for personnel identified as telework-capable. Organizations should work with human resources to support continuing operations in a telework environment. Additionally, organizations should identify necessary accessible methods to maintain effective communication access and telework for employees who are deaf or hard of hearing or employees who are blind or have low vision.

However, telework may not be a viable strategy for continuing essential functions during all incidents, such as cyberattacks and mass power outages. If an organization plans to utilize telework to continue essential functions, planners must document this strategy in its continuity plan. The use of telework may also not work for all organizations or portions of organizations and the effectiveness of this option will be dependent upon factors identified during the BPA. Even if telework may not work for supporting essential functions, it may serve as an option for supporting functions or capabilities necessary to ensure the continued performance of essential functions.

2.3 Devolution

Devolution is the ability to transfer statutory authority and responsibility from an organization's primary operating staff and facilities to other designated staff and alternate locations 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 location unaffected by the incident.

While this option may appear more suited for large federal entities with the option to devolve their operations and essential functions to regional and field offices, it is not exclusive to such organizations. If an incident adversely affects an organization enough that the devolution option must be activated, 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 up 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 could devolve some functions in an effort to alleviate an overwhelming workload upon its personnel during a resource-scarce environment after an incident.



Governments should explore whether or not devolution is a realistic and beneficial strategy. Jurisdictions and non-federal governments may be constrained by laws and regulations, licensing, and liability, which may impact the ability to devolve certain operations. At a minimum, non-federal governments should pursue mutual aid agreements, memorandums of understanding, and contracts with private sector vendors and contractors to supplement or temporarily perform some essential functions under the direction and control of the affected jurisdiction.

When planning for devolution, an organization should consider:

1. The partner to whom performance of essential functions will transfer;
2. 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 authorities and performance of essential functions;
3. How and when direction and control of organization operations will transfer to and from the devolution partner; and
4. The necessary resources, such as personnel, services, equipment and materials, to facilitate the performance of essential functions at the devolution site.

Devolution is a complex continuity strategy that involves planning and training prior to an event. The devolution partner should receive training on:

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

2.4 Mutual Aid Agreements

Because no organization will face a disaster or incident alone, it is incumbent upon the whole community to assist each other. Jurisdictions at all levels should work with each other to develop mutual aid agreements or Emergency Management Assistance Compact (EMAC) procedures.

Mutual aid agreements are a concept that falls under NIMS. Within NIMS, the National Mutual Aid System is built upon the integration of all types of mutual aid into a single system that are most often described by geo-political boundaries including: local, intrastate, regional, interstate, tribal, and international mutual aid. Each level utilizes the levels above, below, and around it to create a unified national system of assistance to ensure a more resilient nation. When local resources are exhausted and resource requests reach the state emergency management agency, the state sources the resource need to intrastate mutual aid, the federal government, the private sector, or EMAC.

Mutual aid agreements already exist in various forms among and between all levels of government. These agreements authorize mutual aid between two or more neighboring communities, between all jurisdictions within a state and between states. Agreements can also be made with and between private sector entities, NGOs, and other partners. The continuity community should consider resources and capabilities across partners and stakeholders and develop written agreements to facilitate access to potentially needed resources.

Step 3: Identify Key Elements

Once options for mitigating the effects of an incident upon the performance of essential functions have been identified, there are a variety of elements that are critical for an organization to execute those options. These elements serve as the foundation of not just how an organization functions during a continuity plan activation, but also 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.

3.1 People

An organization's people are its most valuable resource. Choosing the right people for an organization's staff is always important and is especially true in a crisis situation. Organizations need to consider the impact of threats and



hazards upon the people within its organization. Leadership needs to 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 by an organization's people is dependent upon their safety and social and emotional well-being, to include the statuses of families, pets, service animals, and homes. Continuity plans need to address the emotions and reactions of the people that work within the organization by building preparedness before an incident and care and assistance during and after the incident.

3.1.1 Human Resources

Certain personnel within an organization are needed to continue to perform essential functions during and after the continuity activation. Organizations need to designate such personnel as essential continuity personnel and assign backups to them in case they are unavailable. These individuals may be required to go to alternate locations 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, the designation of employees who are telework-capable to support continuity operations, and those employees that will be excused from duty due to the emergency situation.

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

- Clearly explaining the expectations, roles, and responsibilities to continuity personnel;
- Informing continuity personnel and alternates, in writing, of their roles and responsibilities, as well as ensuring any applicable collective bargaining obligations are satisfied; and
- Maintaining a roster, listing both the primary and alternate continuity personnel, that is regularly updated with contact information.
- Ensuring that the needs of continuity personnel with disabilities are considered during the planning process.

Organizations are responsible for ensuring that continuity planning takes into account personnel with different types of hidden or visible disabilities. During normal operations, a person's disability may not require a reasonable accommodation. However, during an emergency and continuity plan activation, the unpredictability and unstable environment may disproportionately impact personnel with disabilities. To mitigate this effect, organizations should disseminate continuity plans to personnel in advance of an emergency. The process for requesting a reasonable accommodation should be fully articulated within 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:

- **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 or hearing and ensuring electronic materials are compliant with Section 508 – Amendment to the Rehabilitation Act of 1973 so that the materials can be processed effectively by individuals who are blind or have low vision.

- **Accessible facilities and locations.** Organizations are responsible for ensuring the alternate location is accessible to people with disabilities. For people with mobility disabilities, accessibility measures include physically accessible entrances, egresses, restrooms, and paths of travel. Keep in mind that besides people with mobility disabilities, other people may have nonobvious disabilities that require accommodation. For example, people with sensory disabilities, such as people on 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 modification.** Even when an extensive level of accessibility is included in a continuity plan, personnel have the right to request additional reasonable accommodations or modifications of 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 an emergency 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 a continuity plan activation and operations.

Personnel accountability is a critical function for all organizations. Organizations need the means and processes in place to contact and account for employees. Organizations should establish procedures to contact all staff, including contractors, in the event of an emergency to communicate and coordinate activities, provide alerts and notifications, and communicate how, and the extent by which, employees are expected to remain in contact with the organization during an emergency.

The status and operations of an organization is also important to external stakeholders. The organization should develop processes to communicate the organization's operating status to staff and stakeholders; options include establishing a 1-800 hotline or website, announcing via radio or television broadcast, or disseminating via email.

3.1.2 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 dies, resigns, or is otherwise unable to perform the functions and duties of his/her 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 statute, order, or directive.

An organization's legal department or equivalent should develop and review the orders of succession to ensure legal sufficiency. Lawyers can also address legal issues related to rules and procedures officials must follow regarding succession; when succession occurs; the method of notification; and any other limits. Orders of succession include, but are not limited to, leadership, elected officials, and key managers. Establishing an order of succession for

The National Finance Center
Continuity Preparedness and Response

The National Finance Center (NFC) successfully executed its continuity plan in response to a devastating tornado based upon lessons learned from Hurricane Katrina coupled with a robust exercise program. The NFC, a part of the Office of the Chief Financial Officer within the United States Department of Agriculture, is responsible for paying 650,000 federal employees in more than 170 diverse agencies.

After Hurricane Katrina, the NFC staff developed robust continuity of operations plans and integrated continuity training. The staff exercised the continuity plans routinely and established backup capabilities at data centers in other parts of the country. NFC maintains an alternate location in another part of Louisiana, which is capable of hosting hundreds of NFC's 1300 full-time equivalent staff. The NFC exercises the alternate facility at least annually to ensure a high state of readiness.

On February 7, 2017, an Enhanced Fujita scale (EF)-3 tornado, with sustained winds greater than 136 miles per hour, caused severe damage to the NFC facility and displaced 1,300 employees. After the tornado struck, a 50-personnel advance team immediately deployed to the alternate location. The next day, February 8, 2017, more than 130 additional NFC personnel arrived at the alternate location while the majority of NFC employees teleworked. Processing payroll, one of the NFC's essential functions, proceeded without interruption on February 10, 2017. On February 21, 2017, the NFC began reconstituting operations at its primary operating facility in New Orleans. NFC credits effective staff preparedness, including employee familiarity with continuity plans and individual roles and responsibilities, and on-going senior leadership commitment to continuity planning, training, and exercises as key factors in maintaining and implementing its successful continuity capability.

(Note: Our thanks to the NFC leadership for providing the data used in this case study.)

elected officials or organization heads ensures 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 not in direct proximity to the other listed positions.

3.1.3 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 the legal authorization to act on behalf of the organization head or other officials for specified purposes and to carry out specific duties. Delegations of authority will generally specify a particular function that an individual is authorized to perform and includes 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.

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

- 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; and
- Defining the circumstances under which delegation of authorities would take effect and be terminated.

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 delegations of authority are identified as essential records, available during a continuity activation, and updated on a regular basis.

3.2 Technology



Technology is the foundation of many tasks, activities, functions, and capabilities. Information technology is used every day regardless of if or when a threat or hazard is occurring. Individuals 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. The IT/DR plans should be developed in conjunction with an organization's overall continuity plan. Priorities and recovery time objectives for IT capabilities, systems, and services should be identified and developed during the BPA and BIA processes and incorporated into the overall continuity plan. Because technology is continuously evolving, regular review of systems and processes are needed to ensure that the plans do not become obsolete in the face of technological evolution.

3.2.1 Essential Records

All organizations create and manage large volumes of information and data, both in electronic and physical form. Much of that information and data is important. Some of that information and data is essential to the survival and continued function of the organization. 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.

Information systems and applications, electronic and hardcopy documents, references, and records needed to support essential functions during a continuity plan activation are categorized as essential records. Essential records, are 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). Essential records were previously referred to as vital records. Emergency operating records are essential to the continued functioning or recovery of an organization. Legal and financial rights records 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.

Examples of essential records include:

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

Viable continuity programs include comprehensive processes for identifying, protecting, and accessing electronic and hardcopy essential records at primary and alternate locations. Redundant data management software applications and equipment should be standardized throughout the organization and provide the appropriate level of access and cybersecurity to protect sensitive and personally identifiable information, including adhering 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:

- **Using backup servers.** Data and records are backed up on a secondary server, in addition to the primary server. When the backup server is stored in a different location than the primary facility, an organization increases the possibility that data and records are available and accessible.
- **Pre-positioning hard copy records.** Printing hard copy records ensures an organization is not reliant on electronic equipment to access records. Pre-positioning copies at alternate operating locations further protects an organization should the primary facility become inaccessible.
- **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.

3.2.2 Communications



The success of continuity programs is dependent on the availability of and access to communications systems with sufficient resiliency, redundancy, and accessibility available to perform essential functions and provide critical services during a disruption. During an emergency, the ability of a department or agency to execute its essential functions at its primary or alternate location depends on the availability of communications systems. These systems support connectivity among key government leadership, internal elements, other organizations, and the public under all conditions. External communications during a continuity plan activation is an essential function of many organizations during emergencies. External stakeholders and the public will expect information to flow from an affected area and it is vital to an organization that it is able to communicate its status and additional information that is accurate, quick, effective, and accessible to the whole community, including individuals with disabilities and others with access and functional needs.

Organizations should integrate communications contingency needs into continuity planning efforts by incorporating mitigation options to ensure uninterrupted communications support. The risk assessment and BIA identifies 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 its facilities,can ensure communications equipment, such as the switch or the power distribution unit, has strategic sparing of Single Points of Failure, and can confirm geographic separation of primary and alternate transmission media. Communications capabilities must also be interoperable, robust, secure to enable any communications involving sensitive and classified information, and available in sufficient quantity and mode/media commensurate with

each organization's responsibilities in response to a given emergency. 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 locations, devolution, mutual aid agreements, or other mitigation measures are used, organizations should ensure adequate access to and interoperability between communications resources. This includes confirming current copies of essential records, including electronic files and software, are backed-up and maintained off-site.

Potential backup communications options include:

- **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 from 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 wireline or cellular networks.
- **Wireless Priority Service (WPS).** The WPS supports national leadership; federal, state, local, tribal, and territorial governments; and other authorized national security and emergency preparedness users. It is intended to be used in an emergency or crisis situation 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 decreased.
- **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. A TSP assignment ensures that the organization will receive priority attention by the service vendor before any non-TSP service.

3.2.3 Critical Systems



During a detailed BPA, an organization will identify various tasks, functions, and systems important to the continuation of those tasks and 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 and the system impact level. Organizations must account for and utilize various mitigation options for systems that support the organization's operations and assets including those provided or managed by another organization, contractor, or other source. IT/DR plans complement continuity plans, and the two plans should be coordinated. The IT/DR plan impacts an organization's continuity plans and operations by identifying recovery time objectives for key systems that support the performance of functions, including essential functions.

Step 4: Plan and Implement Options and Elements

While an organization needs leaders, staff, communications, facilities, and equipment to perform its essential functions, it also needs comprehensive plans for what to do with those

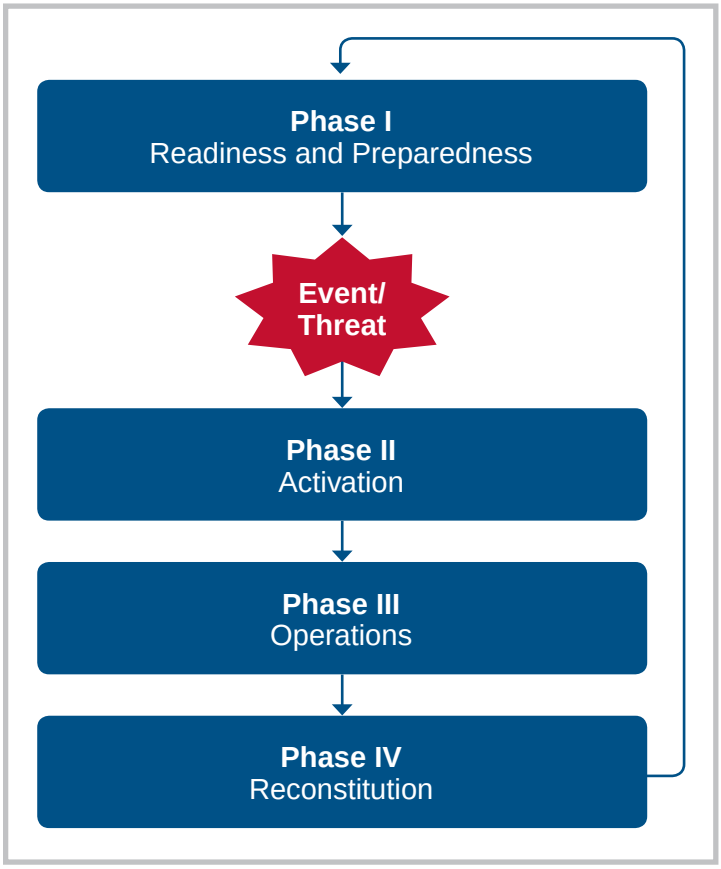


necessary resources. Planning must include considering the requirements and procedures needed to perform essential functions and establishing contingency plans in the event that needed resources are not available.

By continuing the performance of essential functions during and after a catastrophic emergency, federal and non-federal entities support the performance of the NEFs, maintain continuity of government and enduring constitutional government, and ensure that essential services are provided to the Nation's citizens. A comprehensive and integrated continuity program and plan will enable a more rapid and effective response to, and recovery from any emergency, both national and localized.

4.1 Continuity Phases

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 operations: readiness and preparedness, activation, operations, and reconstitution. These four phases should be used to build continuity processes and procedures, to establish goals and objectives, and to support the performance of organizational essential functions during an emergency.



4.1.1 Readiness and Preparedness

Readiness is the ability of an organization to respond to a continuity activation. 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 organization continuity readiness and preparedness activities, including:

1. The development, review, and revision of plans, to include reconstitution and recovery planning;
2. Test, training, and exercise activities;
3. Risk management including identifying mitigation strategies;
4. Incorporation of readiness postures and preparedness measures into daily activities; and
5. Provision of guidance to all staff.

4.1.2 Activation

This phase should include the activation of continuity plans and procedures to enable the continued performance of essential functions. This phase also includes the activation of personnel, essential records and databases, and equipment involved with these functions.

Organizations should outline the process for activating the continuity plan and identify who has authority to activate the plan. An organization may convene a team of senior leadership and/or staff, often called a crisis action team, to review the situation and determine if the continuity plan should be activated.

Organizations should identify triggers to assist leadership in deciding whether or not to activate continuity plans. Triggers assist personnel recognize when continuity plan activation is required and enable a smoother transition to continuity operations. Examples of scenarios that may require activation of continuity plans include:

1. An organization or region receives notification of a credible threat, which leads the organization to enhance its readiness posture and prepare to take necessary actions;
2. An organization experiences an emergency or a disruption to personnel, sites, equipment, or other necessary resources necessary to perform essential functions; and
3. Many, if not all, organizations must evacuate the immediate or geographically affected area.

Organizations should identify roles and responsibilities during continuity activations and operations. 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. Common titles, roles, and responsibilities include:

- **Leadership and elected officials.** The highest ranking official within the organization is usually the individual with the authority to activate the continuity plan. Other senior leaders and subject matter experts may compromise the crisis action team.
- **Crisis action team.** An organization may convene a team of senior leadership and/or subject matter experts, often called a crisis action team, to review the situation and determine if the continuity plan should be activated. This team may also coordinate support and communications among internal and external organizations; initiate personnel accountability to determine the welfare and availability of staff; make recommendations on the activation of associated mitigation strategies within the continuity plan based on the magnitude of the incident and impact on personnel, facilities, and normal business activities; initiate alert and notification of all employees; and ensure essential functions are adequately supported and continued.
- **Continuity personnel.** Continuity personnel, often called the Emergency Relocation Group, are those individuals identified and assigned to perform essential functions and deliver critical services in the event of a continuity plan activation.
- **Reconstitution manager.** The reconstitution manager is an important role within the planning and operational phases. This individual is responsible for planning and managing the recovery of the organization, including facilities, personnel, and systems. Reconstitution is discussed in additional detail in section 4.1.4.
- **All employees.** Because a continuity plan activation impacts the entire organization, all employees are responsible for understanding their roles and responsibilities when the continuity plan is activated.

The activation phase includes the following activities:

1. Occurrence of an incident or the threat of an incident;
2. Deciding to activate the continuity plan when normal operations and necessary resources are impacted;

3. Alerting and notifying personnel, including devolution and mutual aid partners, alternate operating facilities, subordinate and headquarters organizations, all employees, and other stakeholders;
4. Implementing continuity strategies, such as relocating to alternate locations, devolving, or activating mutual aid agreements.

Consideration should also be given to how the organization 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 disaster? 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 essential functions and critical services are not interrupted.

4.1.3 Operations

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

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

4.1.4 Reconstitution

Planning for the recovery of the organization occurs during the readiness and preparedness phase, but the process of reconstitution will generally start when an incident occurs or soon after the incident concludes. During this phase, an organization focuses on returning to normal operations.

Reconstitution occurs on a spectrum with many variables. Reconstitution can be as simple as communicating to stakeholders that offices and facilities will re-open 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 complete destruction of a facility with challenges that include relocating operations, conducting essential functions with survivors, and identifying and outfitting a new permanent operating facility.



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

Some of the activities involved with reconstitution include, but are not limited to:

1. Assessing the status of affected facilities, determining how much time is needed to repair the affected facility and/or to acquire a new facility, and supervising facility repairs;
2. Assessing the status of personnel post-incident to determine their availability to return to work and informing all personnel that the actual emergency, or the threat of an emergency, and the necessity for continuity operations no longer exists, and instruct personnel on how to resume normal operations;
3. Verifying all systems, communications, and other required capabilities are available and operational at the new or restored primary operating facility and that the organization is fully capable of performing all functions, not just essential ones at the new or restored primary operating facility;
4. Implementing a priority-based phased approach to reconstitution by continuing essential functions at the alternate operating facility while non-essential functions return to the new or restored primary operating facility as the organization conducts a smooth transition from one location to the other; and
5. Supervising the return of operations, personnel, records, and equipment to the primary or other operating facility.

Naval Sea Systems Command

Reconstitution after an Active Shooter Incident

On September 16, 2013 an active shooter incident occurred in Building 197 at the Navy Yard in Washington, DC. For two hours, the facility was locked down and personnel sheltered-in-place.

Despite the building remaining intact, personnel did not reoccupy Building 197 until 17 months after the shooting after the Navy completed a $6.4 million renovation of the facility. The renovation made improvements and redesigned the building to ensure it did not resemble the space before and during the shooting. During the renovation, the organization and personnel were temporarily reconstituted at a former Coast Guard facility a few miles away.

When the reconstitution process to return to Building 197 began, there were personnel that refused to return to the facility. The Navy made accommodations for those too traumatized to return and organized small groups of workers to tour the building to ensure that personnel had an opportunity to decide if they were comfortable. Personnel returned on a staggered weekly move-in schedule over nine weeks to ensure full functionality of the facility while minimizing any disruptions to the mission. This event exemplifies the unique considerations and planning required when reconstituting personnel and functions and the importance of leadership commitment and support.

(Note: Our thanks to the Naval Sea Systems Command for providing the data used in this case study.)

FEMA has developed a supporting Continuity Resource Toolkit that provides examples, tools, and templates for implementing each chapter of this Circular. In the future, FEMA will continue to build and distribute tools and information to assist federal and non-federal entities develop and maintain a successful continuity program and plan.

The Toolkit is found at: www.fema.gov/continuity-resource-toolkit.

Continuity Planning Checklist

- ☐ Conduct a BPA to identify and document the activities and tasks that are performed within an organization, with an emphasis on the big picture (how the organization interacts with partners and stakeholders) and the operational details.
- ☐ Conduct a risk assessment to identify and analyze potential threats and hazards.
- ☐ 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.
- ☐ Identify the organization's essential functions and essential supporting activities by determining what organizational functions are essential, taking into account statutory requirements and linkages to National Essential Functions and other essential functions in the community.
- ☐ 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 in the event that key resources are not available.

Chapter 3: Maintaining a Capability

After building a continuity program and plan, organizations, communities, and governments must continue to maintain and improve that capability. Changing threats and resource environments affect continuity strategies and operations. As living documents, plans and policies are continuously updated and refined. This chapter aims to provide guidance and a framework for maintaining a viable continuity capability and maturing a continuity program and plan.



Testing, Training, and Exercising

Test, training, and exercise (TT&E) events assess and validate continuity plans, policies, procedures, and systems. Conducting TT&E events 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 continuity of government and enduring constitutional government plans. To the extent possible, organizations should incorporate continuity aspects into its organization-wide TT&E program rather than developing and conducting stand-alone continuity TT&E events.

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 Federal Continuity Directive 1, 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:

1. Alert and notification systems and procedures for all employees and for continuity personnel;
2. Protection, access, and recovery strategies found in continuity and IT/DR plans for essential records, critical information systems, services, and data;

3. Internal and external interoperability and functionality of primary and backup communications systems;
4. Backup infrastructure systems and services, such as power, water, and fuel;
5. Other systems and procedures necessary to the organization's continuity strategy, such as the IT infrastructure required to support telework options during a continuity plan activation; and
6. Measures to ensure accessibility for employees and members of the public with disabilities.

TRAINING

Training familiarizes individuals with roles, responsibilities, plans, and procedures for conducting essential functions and providing critical services when normal operations are disrupted.

Organizations should train on:

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

EXERCISING

Exercises play a vital role in preparedness by enabling partners, stakeholders, and elected officials to shape planning, test and validate plans and capabilities, and identify and address gaps and areas for improvement. Exercise programs 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:

1. Continuity plans and procedures in order to validate the organization's strategy and ability to continue its essential functions and services;
2. Intra- and interagency backup communications capabilities;
3. Backup data and records required to support essential functions for sufficiency, completeness, currency, and accessibility;
4. Internal and external interdependencies, including support to essential functions and services and situational awareness; and
5. Recovery from the continuity plan activation and environment and a transition back to normal operations.

CONTINUOUS IMPROVEMENT PLANNING

Documenting the strengths, areas for improvement, and associated corrective actions contributes to the strengthening of 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 in future exercises and real-world incidents.

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

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 the moment and is subject to continuous revision.

PLAN REVISION CYCLE

Organizations should periodically review and revise their continuity strategy, plan, and supporting documentation and agreements, to include mutual aid agreements and Memorandums of Understanding (MOUs)/Memorandums of Agreement (MOAs). A cyclical model of planning, training, evaluating, and implementing corrective actions provides leaders and personnel 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 priorities, informs budget decision-making, and drives improvements to plans and procedures as they are revised.

Several factors may affect how often and when an organization, community, or level of government updates its continuity strategy and plan:

- **Change in leadership.** New leadership may want to revise policy, plans, and procedures based upon their experience and history. Newly elected officials and changes to leadership will require updates to orders of succession and delegations of authority.
- **Organizational realignment or re-organization.** An organizational realignment or re-organization may result in changes to essential functions. Rosters, essential records, and other key enablers may then need to be revised.
- **Change in process or system that supports the function.**
- **Results of TT&E events or real-world events and incidents.** TT&E events and real-world incidents can illuminate areas for improvement. Fixing these shortcomings often requires updating plans and procedures.
- **Results of assessments or evaluations.** Assessments and evaluations can also identify areas for improvement, which require changes to plans.
- **Mandated requirements.** Organizations, governments, and standards may set requirements for revision and maintenance schedules. Federal Continuity Directive 1 outlines annual and biennial continuity program maintenance requirements for federal executive branch departments and agencies.

CONTINUITY METRICS

The purpose of a continuity plan and program is to ensure that an organization can perform its essential functions and provide critical services no matter the threat or hazard faced. Developing continuity metrics and then evaluating and assessing continuity plans and programs against these metrics is an important step for planners and managers. Identifying continuity metrics and success criteria assists organizations and communities in determining the viability of the continuity program. Evaluations and assessments against these metrics assist in identifying areas of strength, areas for improvement, best practices, and lessons learned. By examining areas for improvement and areas of strength, organizations can better prioritize and resource continuity needs and gaps.

State of Nebraska

Measuring Continuity Planning and Preparedness

The State of Nebraska has developed a Continuity Scorecard to assist in developing and maintaining state agency continuity plans and providing a status of the state continuity capability to the Governor and Cabinet officials.

The Scorecard, a short evaluation tool, highlights key planning activities and milestones that state agencies should meet when developing and maintaining their continuity plans and programs in support of the overall state continuity program. The evaluation scale identifies planning activities along a spectrum of no continuity plan; limited, moderate, and substantial progress; and objective achieved. Each activity along the spectrum is given a score between 0 and 10, which correlates to an overall red, yellow, or green rating. The State Continuity of Operations Administrator develops a multi-year strategic plan to work with each of the state agencies to improve planning efforts and capabilities.

The continuity capability of each state agency, as identified from the Scorecard, is briefed to the Governor of Nebraska on a monthly basis. The Scorecard and its results enhances state continuity planning by providing regular feedback to the Governor and Cabinet officials on the State's continuity capability, thus enabling leadership support and awareness. A healthy competition has emerged between state agencies to achieve the highest rating on the Scorecard, which further focuses and improves continuity planning within the State.

(Note: Our thanks to the State of Nebraska for providing the data used in this case study.)

An important metric is measuring the ability of an organization to perform its essential functions and be operational in a continuity plan activation. Requirements and standards found in continuity regulations or policy 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 plan and program against the requirements for a viable continuity program and plan as outlined in this document. Within the CAT, there are three sections for evaluation, each of which correspond to the three chapters of the CGC. Each section includes continuity activities and supporting tasks critical to that chapter. These supporting tasks are further divided according to the five solution areas found within the State Preparedness Report: planning, organization, equipment, training, and exercise (POETE). Through this format, an organization can identify its overall progress against the three steps of initiating, building, and maintaining a continuity capability, as well as identify its progress against the POETE elements. The CAT is found within the Continuity Resource Toolkit and should be used on a regular (e.g. annual, multi-year) 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 must align and allocate the resources needed to implement its continuity strategy. Through the budgeting and planning process, an organization's leaders and staff ensures the availability of critical continuity resources needed to continue the performance of the organization's essential functions before, during, and after an emergency or disruption.

Continuity of Operations and Continuity of Government Planning

Statewide Planning within Nevada

The State of Nevada and localities, tribes, and other stakeholders developed a multi-year initiative to develop and update continuity of operations and continuity of government plans and successfully used Homeland Security Grant Program (HSGP) funds to assist implementation.

The Nevada State Homeland Security Strategy identified continuity of operations and continuity of government planning as one of the top three areas of focus when the initiative began. Nevada State law further governs continuity planning within the State by requiring "plans for the continuity of the operations and services of the political subdivision, which plans must be consistent with the provisions of Nevada Revised Statute 239c.260."

In an effort to increase continuity capabilities statewide, a project team developed a multi-year project plan to enhance continuity planning and integrate into existing efforts throughout the State and sustain these efforts in future years. The Nevada Commission on Homeland Security approved the use of HSGP funds to support these efforts. The team developed a continuity task force, comprised of state, local, and tribal government representatives, volunteer agencies, and the private sector, to serve as a steering committee for the effort.

In the first year of the project, the team focused on continuity planning efforts for six counties in the northern part of the state. Subsequent grant cycles enabled extension of the planning effort to the remaining southern and eastern counties while sustaining previous efforts. The HSGP funding used in support of this effort funded task force meetings, planning efforts, and a series of training workshops and resulted in viable continuity plans and templates for jurisdictions throughout the state. In addition, by coordinating participation throughout the State under the limited timeframe of grant funding, the project enabled a cooperative and collaborative approach to continuity planning that leveraged best practices, lessons learned, and shared experiences.

(Note: Our thanks to the State of Nevada; Washoe County, Nevada Emergency Management; and the City of Las Vegas Emergency Management for providing the data used in this case study.)

Once an organization has identified its continuity strategy, including identifying essential functions, conducting a risk assessment, and identifying mitigation options and key elements, an organization 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 test, training, and exercise 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:** Recovering an organization to normal operations may require funding, as will fixing areas for improvement. For example, if the organization used generator fuel during operations, it must fund refilling the supply.

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

1. **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 HSPG. Each government agency sets its priorities for use of grant funding under both programs. Planners and organizations should contact your jurisdiction's grant funding program for additional information and to determine if continuity needs will qualify.
2. **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 a lifecycle replacement, replacing desktop computers with laptops can enable the flexibility and dispersion of an organization. Similarly, upgrades or purchases of some continuity equipment benefit the entire organization; therefore, the cost should be borne by the whole organization rather than one program.
3. **Leverage low- or no-cost resources.** FEMA offers free continuity training, tools, and templates. Virtual training, such as internet-based courses or webinars, also provide a low-cost alternative. Teaming with other organizations through use of mutual aid agreements, EMAC, or MOU/MOAs are low-cost methods of enhancing capabilities.

Multi-Year Strategic Planning

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

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

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

FEMA has developed a supporting Continuity Resource Toolkit that provides examples, tools, and templates for implementing each chapter of this Circular. In the future, FEMA will continue to build and distribute tools and information to assist federal and non-federal entities develop and maintain a successful continuity program and plan.

The Toolkit is found at: www.fema.gov/continuity-resource-toolkit.

Continuity Planning Checklist

- ☐ Establish a schedule for conducting regular test, training, and exercise 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 to evaluate and assess the organization's continuity plans and program against.
- ☐ Establish a schedule for conducting a review (using the continuity metrics and success criteria) and revision of the organization's continuity strategy, plan, and supporting documents and agreements such as Memorandums of Understanding and Memorandums of Agreement.
- ☐ Align and allocate resources (e.g., budget) to implement continuity activities before, during, and following a continuity activation.
- ☐ Develop a continuity multi-year strategic plan to provide for the development, maintenance, and review of continuity capabilities to ensure the program remains viable and successful to include test, training, and exercise activities, and plan reviews.

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 on a daily basis. When an emergency occurs, the need for these services and functions becomes even more critical. Governments and organizations need contingency plans to ensure the performance and provision of these functions and services in the event the emergency disrupts normal operations and necessary resources.



The right people, the right resources, and the right planning helps ensure the continuous performance of essential functions. Continuity cannot be an afterthought. Unfortunately, a myriad of natural hazards and human-caused threats are capable of interrupting 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 time 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 and dangerous, and they could adversely affect the ability of government at all levels and the private sector to provide essential functions and services to citizens. Thus, there is a critical and ongoing need 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 non-government organizations to sustain national essential functions under all conditions.

Appendix 1: Authorities and References

AUTHORITIES:

1. Homeland Security Act of 2002, as amended (6 U.S.C. § 101 et seq.).
2. National Security Act of 1947, as amended (50 U.S.C. § 3042).
3. Telework Enhancement Act of 2010 (5 U.S.C. §§ 6501-6506).
4. Executive Order 12148, *Federal Emergency Management*, July 20, 1979, as amended.
5. Executive Order 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, July 6, 2012.
6. Presidential Policy Directive 8, *National Preparedness*, March 30, 2011.
7. Presidential Policy Directive 40, *National Continuity Policy*, July 15, 2016.
8. Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, February 12, 2013.

REFERENCES:

1. Comprehensive Preparedness Guide 101, *Developing and Maintaining Emergency Operations Plans*, Version 2, November 2010.
2. Comprehensive Preparedness Guide 201, *Threat and Hazard Identification and Risk Assessment Guide*, Second Edition, August 2013.
3. Federal Continuity Directive-1, *Federal Executive Branch National Continuity Program and Requirements*, January 2017.
4. Federal Continuity Directive-2, *Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process*, June 2017.
5. Homeland Security Exercise and Evaluation Program (HSEEP), April 2013.
6. National Incident Management System (NIMS), December 2008.
7. National Preparedness Goal, September 2015.
8. Health Insurance Portability and Accountability Act.
9. Privacy Act of 1974.

Appendix 2: Key Terms

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, and chemical, biological (including pandemic), radiological, nuclear, or explosive events.

Alternate Locations – Fixed, mobile, or transportable locations, other than the primary operating facility, where leadership and continuity personnel relocate in order to perform essential functions following activation of the continuity plan.

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.

Continuity Capability – The ability of an organization to continue to perform its essential functions, using COOP and COG programs and continuity requirements that have been integrated into the organization's daily operations. The primary goal is preserving of our form of government under the U.S. Constitution and the continued performance of NEFs and organizational essential functions under all conditions.

Continuity Coordinator – The 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 manager and other continuity planners within subcomponent levels throughout the organization or government.

Continuity of Government (COG) – 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 Manager – The senior continuity planner responsible for coordinating overall continuity activities within the organization or jurisdiction. This individual managing day-to-day continuity programs, coordinating continuity planners within the organization, representing his/her organization's program externally, as appropriate, and reporting to the continuity coordinator on continuity program activities.

Continuity of Operations (COOP) – An effort within individual organizations to ensure that essential functions continue to be performed during disruption of normal operations.

Continuity Personnel – Continuity personnel, often called the Emergency Relocation Group, are those individuals identified and assigned to perform essential functions and deliver critical services in the event of a continuity plan activation.

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 continuity planner 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 assists the continuity program and planning effort.

Crisis Action Team – A team of senior leadership and/or subject matter experts to 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).

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 manmade, 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, 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 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; an Indian tribe or authorized tribal entity, or in Alaska a Native Village or Alaska Regional Native Corporation; a rural community, unincorporated town or village, or other public entity. See Section 2 (10), Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (2002).

Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) – Written agreements between organizations that require specific goods or services to be furnished or tasks to be accomplished by one organization in support of the other.

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 – It is the policy of the United States to maintain a comprehensive and effective continuity capability, composed of COOP 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 (NEFs) – Select functions necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through COOP, COG, and ECG capabilities.

National Incident Management System (NIMS) – A set of principles that provides a systematic, proactive approach guiding government agencies at all levels, nongovernmental organizations, 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, in order 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 interests of its members, individuals, or institutions. It is not created by a government, but it may work cooperatively with 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. Often these groups 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 manmade 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.

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

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 which 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 associated costs and benefits of any actions taken.

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

Test, Training, and Exercises (TT&E) – Activities designed to familiarize, impart skills, and ensure viability of continuity plans. TT&E aids in verifying that an organization's continuity plan is capable of supporting the continued execution of the organization's essential functions throughout the duration of a continuity plan activation.

Threat – Natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

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; non-profit groups; schools and academia; media outlets; and all levels of government, including state, local, tribal, territorial, and federal partners.

Appendix 3: Acronyms

BIA	Business Impact Analysis
BPA	Business Process Analysis
COG	Continuity of Government
COOP	Continuity of Operations
ECG	Enduring Constitutional Government
EMAC	Emergency Management Assistance Compact
EMPG	Emergency Management Performance Grant
EOP	Emergency Operations Plan
ESA	Essential Supporting Activity
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
MOU	Memorandum of Understanding
NEF	National Essential Function
NGO	Non-Governmental Organization
NIMS	National Incident Management System
PMEF	Primary Mission Essential Function
POETE	Planning, Organization, Equipment, Training, and Exercise
PSTN	Public Switched Telephone Network
THIRA	Threat and Hazard Identification and Risk Assessment
TSP	Telecommunications Service Priority
TT&E	Test, Training, and Exercise
WPS	Wireless Priority Service

Appendix 4: Continuity Planning Checklist

FOREWARD

- [ ] Examine current state of 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 in to integrate continuity planning, operations, and responsibilities into emergency management, preparedness, and resilience efforts.
- [ ] Identify other inter- and intra-organizational continuity plans and programs (e.g., incident management, Occupant Emergency Plans, and Emergency Operations Plans, IT/Disaster Recovery Plans), which should be coordinated with to ensure synchronization across plans and programs.

CHAPTER 1

- [ ] Create an overall continuity strategy that is agreed upon by elected officials or organizational leadership.
- [ ] Identify existing, applicable continuity regulations or requirements. In the absence of requirements, identify continuity guidance, and principles most applicable to the organization.
- [ ] Identify continuity program planning roles and responsibilities.
- [ ] 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.
- [ ] Obtain the support of leadership and elected officials for the continuity program.

CHAPTER 2

- [ ] Conduct a BPA to identify and document the activities and tasks that are performed within an organization, with an emphasis on the big picture (how the organization interacts with partners and stakeholders) and the operational details.
- [ ] Conduct a risk assessment to identify and analyze potential threats and hazards.

  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.
- [ ] Identify the organization's essential functions and essential supporting activities by determining what organizational functions are essential, taking into account statutory requirements and linkages to National Essential Functions and other essential functions in the community.
- [ ] 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 in the event that key resources are not available.

CHAPTER 3

- [ ] Establish a schedule for conducting regular test, training, and exercise 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 to evaluate and assess the organization's continuity plans and program against.
- [ ] Establish a schedule for conducting a review (using the continuity metrics and success criteria) and revision of the organization's continuity strategy, plan, and supporting documents and agreements such as Memorandums of Understanding and Memorandums of Agreement.
- [ ] Align and allocate resources (e.g., budget) to implement continuity activities before, during, and following a continuity activation.
- [ ] Develop a continuity multi-year strategic plan to provide for the development, maintenance, and review of continuity capabilities to ensure the program remains viable and successful to include test, training, and exercise activities, and plan reviews.