



# Federal Continuity Directive

Continuity Planning Framework for the Federal Executive Branch  
FEMA Office of National Continuity Programs

December 2023



FEMA

This page intentionally left blank

# Table of Contents

<b>1. Applicability</b> .....	<b>1</b>
1.1. Scope .....	1
1.2. Distribution .....	1
1.3. Point of Contact.....	1
<b>2. Executive Summary</b> .....	<b>2</b>
<b>3. Background</b> .....	<b>3</b>
3.1. Purpose.....	3
3.2. Policy.....	5
3.3. Essential Functions.....	6
3.4. National Essential Functions.....	7
3.5. Federal and Non-Federal Coordination and Collaboration.....	9
<b>4. Continuity Planning Framework</b> .....	<b>10</b>
4.1. Framework Overview.....	10
4.2. The Four Planning Factors.....	10
4.3. Using the Continuity Planning Framework.....	16
4.4. Continuity and Federal Mission Resilience .....	16
4.5. Resilience Principles .....	17
4.6. Leadership Engagement.....	18
<b>5. Summary</b> .....	<b>20</b>
<b>Annex 1: Authorities and Resources</b> .....	<b>21</b>
<b>Annex 2: Definitions</b> .....	<b>23</b>
<b>Annex 3: Acronyms</b> .....	<b>31</b>

This page intentionally left blank

# 1. Applicability

## 1.1. Scope

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

## 1.2. Distribution

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

## 1.3. Point of Contact

For assistance with the information contained in this FCD, please contact the Associate Administrator, Office of National Continuity Programs (ONCP), Federal Emergency Management Agency (FEMA), at [FEMA-NationalContinuity@fema.dhs.gov](mailto:FEMA-NationalContinuity@fema.dhs.gov).

## 2. Executive Summary

This FCD, *Continuity Planning Framework for the Federal Executive Branch* (hereinafter referred to as the “Framework”), furthers our collective understanding of implementing National Continuity Policy, including the concepts embodied in the *Federal Mission Resilience Strategy* (FMRS).<sup>1</sup> In addition, it establishes a continuity planning framework to assist organizations when considering risk to their essential functions and when creating and maintaining a viable continuity program to achieve Federal Mission Resilience. The four planning factors introduced in this directive—Staff and Organization, Equipment and Systems, Information and Data, and Sites—are necessary to accomplish and manage risk to essential functions. These factors integrate existing doctrine and concepts under a unifying framework to drive resilience and encourage the distribution and diversification of elements involved in an essential function’s performance. Organizational leadership and Mission Owners must integrate continuity into day-to-day operations and empower their personnel at all levels to increase resilience against the disruption of essential functions. Successful sustainment of these functions ensures the continuance of the National Essential Functions (NEFs) and ultimately the continuity of the United States (U.S.) Government.

The threats and hazards we face are real and continue to evolve. They can adversely hinder the ability of government, and the private sector, to provide the Nation with essential functions and services. By maintaining effective continuity capabilities, the Federal Executive Branch continues to advance the goal of a more resilient nation. This occurs by integrating continuity plans and programs to sustain the NEFs under all conditions. Additional FCDs provide guidance and direction on how to apply the Framework to identify and prioritize essential functions, manage the risks to them, and provide the programmatic requirements, standards and processes necessary to build and sustain robust continuity and reconstitution capabilities.

---

<sup>1</sup> Executive Order 13961, *Governance and Integration of Federal Mission Resilience*, 2020.

## 3. Background

### 3.1. Purpose

This Framework is the first in a series of revised FCDs that build upon each other to provide direction and guidance for the Federal Executive Branch.<sup>2</sup> This FCD expands upon federal continuity planning requirements introduced in PPD-40, *National Continuity Policy*; Executive Order (EO) 13961, *Governance and Integration of Federal Mission Resilience*; and FMRS. Federal Mission Resilience concepts within FMRS shift the approach to continuity from an expectation of, and reliance on, timely warning that allows for sufficient lead time to relocate. This new posture encourages using the existing physical and virtual distribution of the Federal Executive Branch while developing additional strategies to increase the resilience of essential functions. This change requires organization leadership and Mission Owners to diligently work with Continuity Coordinators and Continuity Program Managers to use planning, routine decision-making and risk management to ensure resilient essential functions. While relocation of select personnel and operations remains a viable continuity strategy if time allows, increasing the routine use of alternate sites, communications capabilities, distributed staff and leadership will reduce essential function performance downtime.

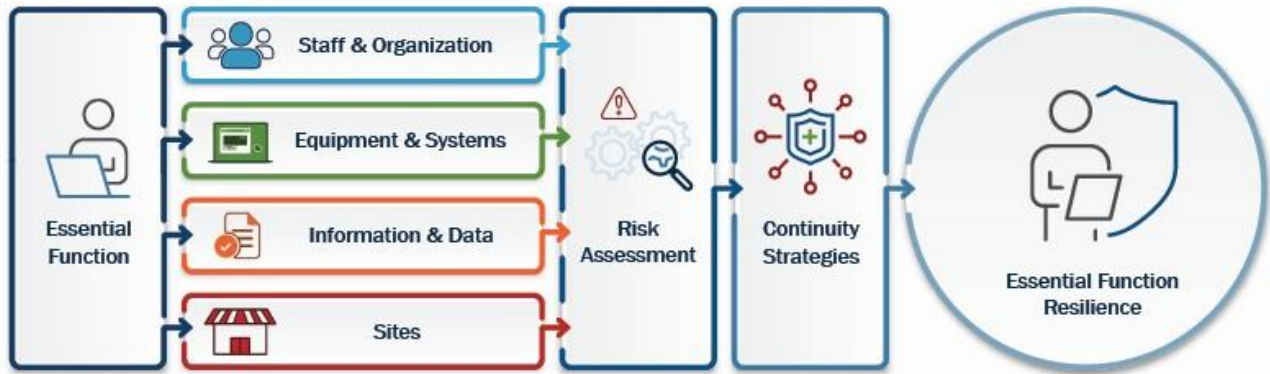
This directive reinforces the Federal Executive Branch organizations' all-hazards approach to continuity planning to manage the consequences of any disruption to normal operations, up to and including incidents or disruptions that occur with little to no warning. It introduces the four planning factors, as outlined in Figure 1, of the Framework:

- Staff and Organization;
- Equipment and Systems;
- Information and Data; and
- Sites.

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

---

<sup>2</sup> The Executive Office of the President and Executive Departments, as defined in 5 U.S.C. 101, government corporations as defined by 5 U.S.C. 103(1), independent establishments as defined by 5 U.S.C. 104(1), the intelligence community as defined by 50 U.S.C. 3003, and the USPS.



**Figure 1: Continuity Planning Framework**

This Framework updates and builds upon existing policy and serves as the foundation for a mission-focused, operational approach to mitigate impacts on these factors from current and future threats and hazards. Additionally, it requires leadership to integrate continuity risk management into day-to-day operations.

Organizations must sustain essential functions during disruptions to normal operations. In the event of a disruption, organizations will likely face limitations on their resources, assets and capabilities. In this constrained environment, functions with little or no allowable downtime will be prioritized over those that can be deferred for longer periods. Organizations must therefore conduct analyses to identify which operations, tasks or functions cannot be interrupted and which may be reduced, deferred or postponed. Organizations prioritize potentially limited resources by understanding the requirements of Staff and Organization, Equipment and Systems, Information and Data, and Sites to accomplish their mission. By considering the vulnerabilities of each planning factor to the full spectrum of threats and hazards, they will better understand the overall risk to each essential function. The distribution of staff, equipment, data and sites is one of many strategies that can mitigate risk and enable organizations to sustain the performance of their essential functions with little to no downtime.

Additional FCDs use this Framework to detail an informed, risk-based approach to decision-making; identify and mitigate negative impacts to essential functions; and help articulate the consequences of failure. They lay out the requirements and standards needed for programs to continue essential functions. Finally, they describe how to reconstitute operations after a disruption that requires the activation of continuity plans.

The FCDs apply to Federal Executive Branch organization headquarters. Organizations are accountable for their essential functions and the associated development of requirements for their subordinate elements. The organization's leadership and Mission Owners will determine the extent to which the principles outlined in the FCDs apply to components, regional offices or field offices. A Mission Owner is an individual accountable for performing an essential function that must be sustained during or quickly resumed following a disruption to normal operations. Leadership must



also consider the organization's regulatory requirements and internal risk management practices. The expected outcome is that essential functions can be continued during or after a disruptive event. Organizations are encouraged to reference the FCDs when publishing supplemental or alternative requirements for their subordinate elements.

## 3.2. Policy

Federal law provides FEMA with the statutory responsibility to serve as the principal advisor to the President for all matters relating to emergency management in the United States and to lead the Nation's efforts to prepare for, protect against, respond to, recover from, and mitigate against the risk of natural disasters, acts of terrorism, and other man-made disasters, including catastrophic incidents.<sup>3</sup> This includes providing federal leadership with the direction necessary for preparing and implementing the federal government's plans and programs for continuity of operations and continuity of government (COG).

EO 12656, *Assignment of Emergency Preparedness Responsibilities*, directs FEMA to serve "as an advisor to the National Security Council on issues of national security emergency preparedness, including mobilization preparedness, civil defense, COG, technological disasters and other issues, as appropriate."<sup>4</sup> The provisions of EO 12656 also state that the FEMA Administrator will:

- Coordinate and support the initiation, development and implementation of national security emergency preparedness programs and plans among Federal departments and agencies;
- Coordinate the development and implementation of plans for the operation and continuity of essential domestic emergency functions of the Federal Government during national security emergencies; and
- Support the heads of other Federal departments and agencies in preparing plans and programs to discharge their national security emergency preparedness responsibilities, including, but not limited to, such programs as mobilization preparedness, continuity of government planning, and continuance of industry and infrastructure functions essential to national security.

PPD-40, *National Continuity Policy*, outlines the overarching continuity requirements for the Federal Executive Branch and directs the Secretary of Homeland Security, through the FEMA Administrator, to coordinate the implementation, execution and assessment of continuity activities among Federal Executive Branch D/As. Specifically, it directs the FEMA Administrator to develop and publish FCDs to establish continuity program and planning requirements that:

---

<sup>3</sup> Homeland Security Act of 2002, Secs. 503-504, 6 U.S.C. §§ 313-314.

<sup>4</sup> Executive Order 12656 – Assignment of Preparedness Responsibilities - The Executive Office of the President and Executive Departments, as defined in 5 U.S.C. 101, government corporations as defined by 5 U.S.C. 103(1), independent establishments as defined by 5 U.S.C. 104(1), the Intelligence Community as defined by 50 U.S.C. 3003, and the USPS.

- Coordinate the implementation, execution and assessment of continuity operations and activities among Federal Executive Branch D/As;
- Develop and promote FCDs to establish continuity program and planning requirements for Federal Executive Branch D/As;
- Conduct biennial assessments of individual D/A continuity capabilities;
- Develop, lead and conduct a federal continuity training and exercise program; and
- Develop and promote continuity planning guidance for state, local, tribal and territorial (SLTT) governments, nongovernmental organizations (NGOs) and private sector critical infrastructure owners and operators.

In 2020, the President issued EO 13961, *Governance and Integration of Federal Mission Resilience*, and the FMRS. EO 13961 details a comprehensive approach to integrating continuity and enterprise risk management to increase the resilience of the day-to-day operations of the Federal Executive Branch.

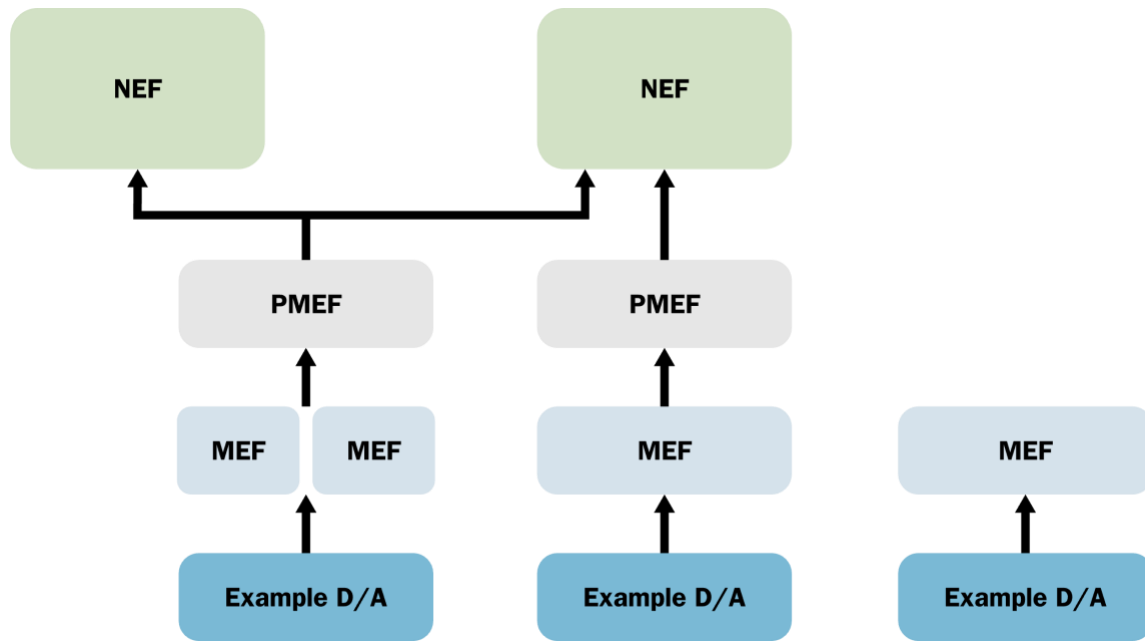
This Framework aligns with the FMRS to support the federal government's increasing resilience against all threats through an enduring structure of distributed risk and enhanced continuity capabilities.

### 3.3. Essential Functions

The *National Continuity Policy* establishes a tiered approach to operational activities for the Federal Executive Branch. This starts with government functions, which are the collective functions of the Federal Executive Branch as defined by statute, regulation, presidential directive or other legal authority. The criticality of some identified Federal Executive Branch functions for accomplishing agency and national-level missions makes them essential.

As defined by PPD-40, essential functions are subsets of those government functions and are categorized as Mission Essential Functions (MEFs), Primary Mission Essential Functions (PMEFs) and NEFs.

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



**Figure 2: MEF, PMEF and NEF Alignment**

Not all organizations have PMEFs that directly support or implement one or more of the NEFs, as depicted in Figure 2. Organizations with PMEFs that support or implement NEFs generally require more substantial capabilities to ensure the resilience of those functions so that the NEFs are not negatively impacted. Organizations that do not have PMEFs that support or implement the NEFs must still ensure the ability to perform their essential functions in accordance with the unique performance requirements of each. Other FCDs clarify how to identify and assess essential functions for resilience.

### 3.4. National Essential Functions

As established in PPD-40, “It is the policy of the U.S. to maintain a comprehensive and effective continuity capability through [continuity of operations], COG, and ECG programs, ensuring the resilience and preservation of government structure under the U.S. Constitution and the continuous performance of NEFs under all conditions.”<sup>5</sup> National-level coordination of effort enables the continuous performance of NEFs; therefore, their performance and associated risk mitigation require coordinated efforts across the whole community, generally including the whole of government as well as private and nonprofit entities.

<sup>5</sup> Presidential Policy Directive - 40, *National Continuity Policy*, 2016.



**Figure 3: NEFs**

To sustain the NEFs, organizations must identify MEFs and PMEFs and establish programs that ensure the functions' resilience to disruption. Identification and prioritization of essential functions are the foundation of continuity planning; they establish the parameters that drive an organization's continuity planning and preparedness efforts. NEFs and the organizational essential functions that support them represent the overarching responsibility of the federal government to lead and sustain the Nation.

Within each of the executive, legislative and judicial branches, COG is the coordinated effort to ensure that governance and essential functions continue to be performed. This is an outcome of viable continuity programs and organizations mitigating risk and collectively sustaining their organizational essential functions.

By extension, ECG is the cooperative effort among the executive, legislative and judicial branches to preserve the constitutional framework under which people are governed. ECG focuses on the ability of all three branches of government to execute constitutional responsibilities under all conditions.

- Continuity of operations ensures that essential functions can be performed.
- COG ensures the integrated performance of essential functions by a branch of government.
- ECG safeguards the functionality of all three branches of government.

Because essential functions are interdependent, organizations and offices must support and coordinate across all levels of government and create partnerships with the private sector.

## 3.5. Federal and Non-Federal Coordination and Collaboration

Continuity is not strictly the responsibility of the federal government. It reaches across all federal and SLTT communities, the private sector, and individuals. Leadership must consider these communities based on their unique missions and operations. Organizations must engage with partners, stakeholders, coordinating entities and service providers within their organization and externally to integrate continuity plans. Organizations must coordinate continuity plans and programs with their operational plans, such as incident management plans, Occupant Emergency Plans and other emergency operations plans. Proper testing, training and exercising help delineate roles and responsibilities and resolve procedural, resource and personnel issues. That effort is critical to developing and sustaining continuity capabilities that are meaningful, effective and foundational for the safety, security and continuation of our Nation's government.

Collaboration among federal organizations, non-federal organizations and the private sector is not without its challenges. For example, federal and non-federal governmental organizations rely on fuel from the private sector to power equipment such as vehicles and generators. In an emergency, a very small number of vendors, faced with limited access to a potentially interrupted supply of product, will cause widespread disruptions to both life-sustaining activities and government operations. This complex challenge must be addressed through engagement that establishes relationships, recognizes the priorities of federal and non-federal stakeholders and creates a better understanding of private sector infrastructure systems.

Utilizing the delegated authority of the FEMA Administrator to lead D/A continuity activities in the executive branch, the Associate Administrator for the Office of National Continuity Programs at FEMA has established and chairs the Continuity Advisory Group (CAG). The CAG serves as an interagency forum to address all aspects of Federal Executive Branch review and implementation of national continuity policy, planning, operations, exercise, assessment and evaluation. It also shares best practices and lessons learned in the implementation of national continuity policy and the furtherance of Federal Mission Resilience.

Additionally, Interagency Continuity Working Groups (ICWGs), chartered by the CAG, enable Federal Executive Branch Continuity Program Managers to collaboratively review, assess, prepare for and implement the requirements outlined in current and future national continuity and Federal Mission Resilience policy.

Organizations must create partnerships to coordinate the use of resources and increase their day-to-day continuity capabilities. Continuity coordination meetings promote the development, coordination, funding and integration of continuity planning and programs within the Federal Executive Branch and can facilitate further collaboration with non-federal organizations and the private sector.

## 4. Continuity Planning Framework

### 4.1. Framework Overview

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

To enhance continuity capabilities and Federal Mission Resilience, organizations must adopt a program focused on resource impacts, regardless of the nature of threats or hazards that caused them. Resilience can occur through the distribution of the function the risk is impacting. Organizations can use the four planning factors to mitigate risk with a solid understanding of the dependencies or interdependencies of each essential function’s resource requirements.

### 4.2. The Four Planning Factors

The Framework’s four planning factors help organizations consider the dependencies of and risks to their essential functions’ development and maintenance of a viable continuity program.

- **Staff and Organization:** Staff within an organizational structure who are required to individually and collectively support or perform the essential function.
- **Equipment and Systems:** Physical resources or digital applications required to support the accomplishment of the essential function.
- **Information and Data:** The information and data required to complete the essential function or that result from its completion.
- **Sites:** The facilities needed to coordinate or accomplish the essential function.

#### 4.2.1. Staff and Organization

People are the most valuable resource in any organization. Leadership, including Mission Owners as well as management and staff (both government employees and contractor personnel), must be organized to support decision-making and the performance of essential functions. During a disruption to normal operations, organizations mobilize specific, pre-identified personnel as necessary to sustain essential functions. These continuity personnel or teams can be known as the Emergency Relocation Group (ERG), the Devolution



#### Staff and Organization

Who in the organization’s leadership is required to perform the task, if direct leadership involvement is needed?

What staff are required to directly support or perform the essential function (including specific skill sets, expertise and authorities needed)?

Emergency Response Group (DERG), Out of Area Successors or other organizational terms to indicate their critical nature in the continuance of essential functions.

**Emergency Relocation Group:** Staff assigned to physically relocate and continue the performance of essential functions at an alternate location in the event that their primary operating facility or facilities are impacted or incapacitated by an incident.

**Devolution Emergency Response Group:** Personnel stationed at a geographically distant location, not the primary location, who are identified to take over for primary site personnel and continue the performance of essential functions.

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

However, all organizational personnel, not just those identified per PPD-40 as continuity personnel, should be viewed as resources that should be relied upon. These personnel may be asked to support operations from an organization's alternate site or another directed work location (e.g., alternate worksites, telework, remote work), maximizing workplace flexibilities. Organizations should therefore provide guidance on individual preparedness to mitigate risk to all their personnel. Organizations must consider any additional equipment, transportation costs, and data access needs at directed worksite locations, particularly if they are reliant on commercial infrastructure (e.g., water, power, communications). Organizations may increase their workforce capacity by collaborating with staff at partner locations or other geographically distributed locations. For example, they may cross-train personnel to ensure that staffing issues do not affect the organization's ability to perform essential functions.

Resilience is ultimately the responsibility of the organization's leadership. Leadership must develop and provide resources for continuity programs that can maintain essential functions while accounting for other requirements resulting from the emergency or event, such as personnel protection. Organizations must ensure there is always a senior official with proper authority in place should rapid changes occur. Maintaining leadership continuity during any level of disruption is critical. Robust orders of succession and delegations of authority ensure that the organization has identified key personnel to assume leadership positions and decision-making authority when needed.

## 4.2.2. Equipment and Systems

Organizations must plan for every physical resource or digital application resource they require to perform their operations. Further, these resources are more resilient when there are redundant options to perform operations across geographically dispersed locations. The availability of usable computers, servers, software, communications devices and other physical assets is key to the successful sustainment of essential functions. However, equipment and systems are not exclusively communications- or information technology (IT)-based physical assets. Vehicle fleets (aircraft, government vehicles, forklifts, etc.) may also be needed to ensure continuity.



### Equipment and Systems

What communications, IT equipment and software are required to support the task (including any unique or unusual requirements)?

What supplies, services and capabilities (not already addressed) are required to perform the task (including the ability to obtain, purchase and relocate these resources)?

These assets must be properly secured and located at sites with appropriate personnel access and other security precautions, which may include physical hardening (employing measures to protect assets from the impacts of threats and hazards). Equipment and systems must be considered separate from the information and data that may be housed within them so that the loss of or degradation of equipment and systems does not impact organizational information and data, or vice versa. Primary, Alternate, Contingency, Emergency (PACE) communications planning in general is used to mitigate risk and enhance resilience by developing several fallback plans that ensure the communication needed to accomplish essential functions. It designates the order in which an organization or element will move through available communications systems until contact can be established with the desired distant element. All personnel required to operate essential equipment and systems must be properly trained and understand the PACE methodology.

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


Minimum communications requirements are found in the Office of Science and Technology Policy/Office of Management and Budget Directive D-16-1, *Minimum Requirements for Federal Executive Branch Continuity Communications Capabilities*, its amendments, and the additional FCDs.



### 4.2.3. Information and Data

Access to information (data in a usable form) and data (a set of values that presents facts, concepts or instructions in a formalized manner) is critical to the continued performance of an organization's essential functions. Planning for the resilience of information and data is often unique to each individual system, considering preventative measures, recovery strategies and technical considerations appropriate to classification level, confidentiality, integrity and availability requirements. Procedures must be established for personnel to access the information and data they require, regardless of where operations are occurring. All organizations are responsible for ensuring that third-party data providers provide secure, consistent and redundant access to networks and data but must also account for the loss of commercial services by maintaining and protecting the data stored on their systems. Organizations must plan for the physical loss and degradation of the equipment and systems, or software used to access the data, independent of the loss or degradation of the information and data themselves.

Organizations, regardless of size, must implement strategic decisions that improve cybersecurity posture and take steps to reduce the likelihood of a damaging loss of information. Organizations should have multiple copies of their essential records in several locations stored on redundant media and in virtual storage environments. Essential records are defined as "records (emergency operating records) to protect the legal and financial rights of the government and those affected by government activities (legal and financial rights records)."<sup>6</sup> Organizations can consult resources provided by the National Archives and Records Administration (NARA) for information about essential records and records recovery after a disaster or an emergency event.<sup>7</sup> Hardening measures to protect the organization's data, such as data redundancy, encryption and strict access controls, must be implemented to mitigate risks that may impact the performance of essential functions. These actions should apply to physical servers that house critical information and data as well as software, applications and networks. Taking these steps will enable an organization to quickly detect a potential intrusion and ensure that it is prepared to respond and protect its most critical assets against a disruptive cyber incident.

 Information and Data

What information and data are required for this task, from both internal and external partners?

What information and data result from the performance of this task (including metrics that identify specific performance measures and standards)?

---

<sup>6</sup> Title 36, *Code of Federal Regulations*, Part 1223.2.

<sup>7</sup> [Essential Records Information | National Archives](#)

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

Organizations can improve their cyber resilience through deliberate cybersecurity risk management activities. The Cybersecurity and Infrastructure Security Agency (CISA) urges cybersecurity/IT personnel to regularly review organizational threats and destructive exploits against critical infrastructure. CISA's Shields Up campaign webpage provides recommendations, products and resources to increase organizational vigilance and keep stakeholders informed about cybersecurity threats and mitigation techniques.<sup>8</sup> The complementary Shields Ready campaign webpage provides guidance for critical infrastructure organizations to identify critical assets and map dependencies, develop plans and exercise capabilities, and implement program evaluation and improvement activities to reinforce readiness.<sup>9</sup> The National Institute of Standards and Technology (NIST) has also published a cybersecurity framework, which provides a methodology for organizations to improve their cybersecurity posture and manage cybersecurity risk.<sup>10</sup>

#### 4.2.4. Sites

Primary sites are where organizations perform the day-to-day operations of either or both their essential functions and command and control functions. Organizations must identify alternate sites that are unlikely to be affected by the same disruption or incident that drives operations away from the primary site. At these alternate sites, personnel must have access to the equipment, systems, software, information and data needed to perform essential functions until the organization can reconstitute to a repaired or new facility. Organizations must conduct risk assessments on all operating facilities—primary and alternate—to evaluate the impacts of disruptions caused by threats or hazards on the conduct of essential functions.<sup>11</sup>



#### Sites

What are the facility requirements for performing the task (e.g., facility type, square footage, security, infrastructure required)?

Is the alternate site at a sufficient distance from the primary facility, and not susceptible to the same risks associated with the primary facility?

<sup>8</sup> [Shields Up: Guidance for Organizations | Cybersecurity and Infrastructure Security Agency \(cisa.gov\)](#)

<sup>9</sup> [Shields Ready | Cybersecurity and Infrastructure Security Agency \(cisa.gov\)](#)

<sup>10</sup> *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, 2018.

<sup>11</sup> The Interagency Security Committee establishes requirements, frequency and standards for conducting facility risk assessments per its authority under Executive Order 12977.

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

While hardening and using alternate sites remain valid continuity strategies to mitigate many threats and hazards, the distribution of operations is encouraged and complements other strategies like relocation. Distributing operations, along with reducing single points of failure, requires the use of scalable, flexible and adaptable operations techniques across separated geographic areas. The goal of distributed operations is to reduce overall risk and the likelihood of impacts to essential functions while acknowledging that not every operation can be distributed and residual risk may be transferred to other areas.

When distributing operations, organizations should consider using existing organizational and partner facilities to effectively reduce downtime of essential functions. This strategy distributes risk to the performance of essential functions, services and operations and minimizes or mitigates single points of failure. Collaborating and coordinating with other organizations can lead to creative solutions for enhancing the resilience of each organization's missions and operations. For example, identifying opportunities for the shared use of a resource (e.g., a facility that provides classified communications capabilities) through the execution of memoranda of agreement/understanding, standing visit access requests, reciprocity and interagency agreements is encouraged wherever possible.

Organizations must also plan for situations where facilities may be degraded or made inaccessible for varying lengths of time. An organization's ability to distribute its regular operations across geographically separate locations that are less likely to be affected by the same disruption increases the likelihood that it can successfully continue its essential functions under any conditions and ensure Federal Mission Resilience. It is important to note that with hardened infrastructure, relocation and devolution capabilities support and complement distributed operations by providing leaders with more personnel and location options to continue performing essential functions. Telework and remote work can provide additional flexibility in situations where commercial infrastructure is still functional. The COVID-19 pandemic demonstrated that many organizations could sustain their operations using telework and remote work.

Although the process for identifying and selecting one or more physical locations differs between organizations, it must be based on their unique missions and operations and the results of holistic organizational risk assessments. No matter where organizations conduct operations, they must ensure that personnel can access a site with the equipment, systems and data needed to accomplish the mission.

## 4.3. Using the Continuity Planning Framework

Organizations will use this Framework’s planning factors to understand vulnerabilities and determine where to develop and invest in risk mitigation strategies. They will also use the Framework, along with additional FCDs, to understand the resources and actions required for essential functions to continue during a disruption. This will enable them to reduce or mitigate the consequences of threats, hazards and vulnerabilities.

As organizations identify and prioritize functions, they must treat the Framework’s planning factors as separate, related aspects of their operations. The organization must apply the Framework across all the functions it performs, as the Staff and Organization, Equipment and Systems, Information and Data, and Sites for one organizational function may not be impacted by an incident affecting a different function. Mitigation actions will vary between different organizations, functions and incidents. The ability to modify mitigation actions enables organizations to easily adapt their decision-making when addressing operational impacts.

Specific strategies include, but are not limited to, hardening, workplace flexibilities, directed work locations, distribution, relocation and devolution. Organizations should develop plans with multiple options for the seamless continuation of essential functions as the situation, mission and functions require.

To stay relevant in an ever-changing risk landscape, continuity strategies must be informed by and adjust to the results of periodic assessments, such as the biennial essential function review process and exercise or event after-action reviews. As continuity strategies evolve and greater emphasis is placed on the distribution of operations, organizations must continue to provide sufficient resources to ensure that all planning factors—Staff and Organization, Equipment and Systems, Information and Data, and Sites—are available when needed.

The Framework enables flexibility and adaptability for organizations with varying needs and capacities and aligns resources with the execution of plans and procedures. It is based on the idea that organizational continuity responsibilities are not separate and compartmentalized roles. To sustain operations and functions in an all-hazards environment, organizations must establish and resource continuity programs to ensure that plans can be executed. Application of the Framework is an inherent part of daily operations that allows organizations to achieve and maintain day-to-day Federal Mission Resilience.

## 4.4. Continuity and Federal Mission Resilience

For organizations to achieve Federal Mission Resilience, leaders must commit to and sustain attention on continuity planning. They must also fully integrate continuity principles into the organization’s everyday operations. This leadership engagement—along with a routine organizational focus on risk management, budget considerations, IT systems, physical locations and staffing

considerations—is essential. Effective implementation of continuity plans and programs requires the support of leaders who have the authority to commit the organization and the resources required to achieve the resilience of essential functions. Organizations should also prioritize investments that improve Federal Mission Resilience, including the investment of resources and tools that mitigate challenges and control identified gaps.

“Federal Mission Resilience is the ability of the Federal Executive Branch to continuously maintain the capability and capacity to perform essential functions and services, without time delay, regardless of threats or conditions, and with the understanding that adequate warning of a threat may not be available. Federal Mission Resilience will be realized when preparedness programs, including continuity and enterprise risk management, are fully integrated into day-to-day operations of the Federal Executive Branch.”<sup>12</sup>

Sustaining essential functions requires identifying measurable, data-driven, flexible risk mitigation options that address threats and hazards through an informed decision-making process. Decision-makers will use this Framework and additional directives when considering the feasibility of implementing strategies to reduce risk to essential functions. Continuity planning should not occur in a vacuum; it must include all aspects of an organization’s internal and external operations.

## 4.5. Resilience Principles

The focus of a successful continuity program is the organization’s mission and the functions that support it. Organizational leadership, Continuity Coordinators, Mission Owners and Continuity Program Managers must collaborate to develop resilient essential functions using the following principles:

- Identify the processes, resources and dependencies that support organizational functions and operations, and apply appropriate continuity strategies using this Framework;
- Prioritize investments that improve resilience, including investments that mitigate acknowledged challenges, and close self-identified gaps;
- Through tests and exercises, assess and validate continuity policies, plans, procedures and operational capabilities;
- Train all personnel at all levels within an organization to ensure they understand how to execute their assigned operational role in any environment;
- Document the use of plans during tests, exercises and real events by conducting after-action reviews and implementing corrective action efforts that address gaps and shortfalls in plan execution; and

---

<sup>12</sup> *Federal Mission Resilience Strategy*, 2020.

- Ensure that continuity strategies are incorporated as a fundamental part of daily operations so that operational success is achieved and essential functions continue.

## 4.6. Leadership Engagement

Leaders are directly responsible when services are not delivered or functions are not performed. Therefore, they must commit to developing and maintaining their organization's continuity capabilities. Achieving Federal Mission Resilience requires leadership and continuity programs to mitigate challenges, threats and hazards. Leaders must engage Continuity Program Managers to integrate and identify resources necessary to sustain operations and support continuity operations through the continuation of essential functions. This commitment must include a comprehensive planning effort in which continuity and emergency plans are coordinated and integrated with day-to-day operations and are understood and executable by internal staff and external stakeholders. Additionally, both plans and operations must be developed, coordinated, implemented, trained and validated through robust exercises.

Leadership must ensure that each part of the organization is involved in the planning effort and held accountable in order to achieve effective continuity. Each part of the organization must buy into and participate in continuity and risk management efforts to effectively ensure resilience across the organization. Leadership engagement is especially important because, unlike the organization's Continuity Program Manager, senior leaders typically have the authority to direct such engagement, inform budget priorities, and hold personnel across the organization accountable. Leaders at the Secretary and Deputy Secretary (or equivalent) levels are required to engage directly to ensure the resilience of essential functions and to make sure that Federal Mission Resilience remains at the forefront of all intra- and interagency efforts.

Organizations should leverage a concept such as Planning, Programming, Budgeting and Execution (PPBE) to allocate resources, make decisions and communicate program priorities. PPBE is an annual process focused on financial and resource management comprised of four interconnected phases:

- **Planning:** As a short- and long-term effort, organizations define and articulate strategies to inform operational activities and programmatic resource planning. This phase allows continuity programs to assess changing threat, technology and economic conditions and to illustrate the short- and long-term budget and strategic planning implications.
- **Programming:** The process to translate organizational priorities and strategic guidance into specific resource allocation decisions over a multiyear period. This phase allows continuity programs to define and analyze investments, construction, human capital, IT and other support and operating expenses with their multiyear resource implications and the evaluation of various trade-off options.
- **Budgeting:** The process to develop a budget submission, including the formulation, justification, execution and control of the budget to organizational leadership and budget approval bodies.

The purpose is for organizations to acquire the resource funding needed to ensure the resilience of essential functions.

- **Execution:** The process by which organizations dispense resources and identify cost and performance monitoring to determine the value and impact of essential functions performance. Organizations will regularly review and report expenditures to ensure alignment to strategic and leadership priorities.

Mission Owners must be actively involved in and committed to essential function resilience. For the Federal Executive Branch, this is the senior accountable government position with the original or delegated authority to lead PPBE and associated risk management of a specific essential function.

PPD-40 requires the appointment of a Continuity Coordinator at the Assistant Secretary level. The Continuity Coordinator may appoint a Continuity Program Manager to oversee the day-to-day management of the continuity program(s). As the organizational official responsible for coordinating with internal organizational leaders and national continuity leadership, the Continuity Coordinator must, among other requirements:

- Represent the organization on the Continuity Advisory Group;
- Work with other organizations to identify and understand the organization's PMEFs and MEFs; and
- Advocate for the continuity program within the organization.

The Continuity Coordinator should be meeting with their Deputy Secretary (or equivalent) regularly, at minimum quarterly, to discuss internal continuity matters and mission resilience. During these meetings, they should also identify, as necessary, risks with the potential to impact or disrupt enterprise essential functions operations and continuity programs, as well as issues affecting their department or agency and the resources needed to support those functions and programs.

If the role is established within an organization, a Continuity Program Manager must, among other requirements, work with the rest of the organization to:

- Coordinate and manage activities enabling the performance of essential functions during any disruption to normal operations;
- Facilitate the development and update of the continuity plan(s); and
- Assist in the identification and budgeting of the needed resources.

An organization's leadership and Mission Owners must leverage the Framework and additional FCDs to further integrate continuity into day-to-day operations and empower Continuity Program Managers and all other personnel to assure resilient essential functions. By maintaining these functions, organizations collectively provide for the continuance of NEFs and the continuity of the U.S. Government.

## 5. Summary

Implementing a unifying framework across the department or agency will enable leadership to increase resilience and improve their organizations' continuity capabilities. FEMA will provide future updates to better align the continuity doctrine—including the four interconnected planning factors: Staff and Organization, Equipment and Systems, Information and Data, and Sites—with policy changes and best practices. The doctrine will continue to address evolving threats and hazards through adaptive all-hazards planning and the practical implementation of continuity programs. The key to achieving these objectives is leadership engagement. Each organization's leadership is responsible for their own functions, as outlined in their individual authorities. Continuity of these responsibilities should therefore be a daily priority for each organization at all levels of operation.

Going forward, the FCDs will continue to improve based on real-world experience, with data-driven evidence driving change and encouraging continual process improvement. Additional FCDs provide guidance and direction on how to apply the Framework to identify and prioritize essential functions and the programmatic requirements, standards and processes necessary to build and sustain robust continuity and reconstitution capabilities.



# Annex 1: Authorities and Resources

## AUTHORITIES

1. Homeland Security Act of 2002, as amended (6 United States Code [U.S.C.] § 101 et seq.).
2. National Security Act of 1947, as amended (50 U.S.C. § 3042).
3. Vacancies Reform Act of 1998, as amended (5 U.S.C. §§ 3345–3349d).
4. Telework Enhancement Act of 2010 (5 U.S.C. §§ 6501–6506).
5. Executive Order 12148, *Federal Emergency Management*, as amended, July 20, 1979.
6. Executive Order 12656, *Assignment of National Emergency Preparedness Responsibilities*, November 18, 1988.
7. Executive Order 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, July 6, 2012.
8. Executive Order 13961, *Governance and Integration of Federal Mission Resilience*, December 7, 2020.
9. Presidential Policy Directive 8, *National Preparedness*, March 30, 2011.
10. Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, February 12, 2013.
11. Presidential Policy Directive 40, *National Continuity Policy*, July 15, 2016.
12. *Federal Mission Resilience Strategy*, December 7, 2020.

## RESOURCES

1. Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements*, June 2017.
2. Federal Continuity Directive 2, *Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process*, June 2017.
3. *Continuity Guidance Circular*, February 2018.
4. National Institute of Standards and Technology Interagency Report 7298 Revision 3, *Glossary of Key Information Security Terms*, July 2019.
5. National Institute of Standards and Technology Interagency Report 8286, *Using Business Impact Analysis to Inform Risk Prioritization and Response*, November 2022.
6. Executive Order 12977, *Interagency Security Committee*, October 19, 1995, as amended.

7. Office of Science and Technology Policy/Office of Management and Budget Directive D-16-1, *Minimum Requirements for Federal Executive Branch Continuity Communications Capabilities*, December 2016.
8. Cybersecurity and Infrastructure Security Agency, [Shields Up: Guidance for Organizations](#).
9. Cybersecurity and Infrastructure Security Agency, [Shields Ready](#).
10. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, April 2018.
11. Department of Homeland Security, *Lexicon Terms and Definitions*, 2017.
12. Title 36, Code of Federal Regulations, Part 1223—*Managing Vital Records*.
13. National Archives and Records Administration, *Essential Records Information*, 2020.

## Annex 2: Definitions

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

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

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

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

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

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

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

**Continuity Coordinators** – Senior accountable executive branch officials at the Assistant Secretary or equivalent level who represent their departments and agencies (D/As) on the CAG, ensure continuity capabilities in the organization, and provide recommendations for continuity policy. Continuity Coordinators are supported primarily by the Continuity Program Manager and by other continuity planners or coordinators at their subordinate levels throughout their organizations (Source: FEMA).

**Continuity of Government** – “A coordinated effort within the executive, legislative or judicial branches of the U.S. Federal Government to ensure that NEFs continue to be performed during a catastrophic emergency” (Source: PPD-40, *National Continuity Policy*).

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

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

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

**Continuity Program Manager** – The Senior Continuity Planner responsible for managing day-to-day continuity programs, representing his or her department or agency on the CAG and working groups, as appropriate, and reporting to the Continuity Coordinator on all continuity program activities (Source: FEMA).

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

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

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

**Devolution** – The transfer of statutory authority and responsibility from an organization’s primary operating staff and facilities to other staff and alternate sites to sustain essential functions when necessary (Source: FEMA).

**Devolution Emergency Response Group** – Personnel stationed at a geographically distant location, not the primary location, who are identified to take over for primary site personnel and continue the performance of essential functions (Source: FEMA).

**Digital Applications** – A software system or program implemented to satisfy a particular set or subset of requirements. The term “application” is generally used when referring to a component of software that can be executed (Source: National Institute of Standards and Technology).

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

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

**Emergency Relocation Group** – Staff assigned to physically relocate and continue the performance of essential functions at an alternate location in the event that their primary operating facility or facilities are impacted or incapacitated by an incident (Source: FEMA).

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

**Essential Functions** – “Subsets of government functions that are categorized as MEFs, PMEFS [Primary Mission Essential Functions] and NEFs” (Source: PPD-40, *National Continuity Policy*).

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

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

**Federal Continuity Directive** – A continuity enterprise document developed and promulgated by the FEMA Administrator, in coordination with the CAG and in consultation with the ICWG, that directs

executive branch organizations to carry out identified continuity planning requirements and assessment criteria (Source: FEMA).

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

**Government Functions** – The collective functions of the EOP and D/As as defined by statute, regulation, presidential direction or other legal authority, including the functions of the legislative branch and judicial branch (Source: PPD-40, *National Continuity Policy*).

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

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

**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 (Source: FEMA).

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

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

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

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

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

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

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

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

**Nongovernmental Organization** – An entity with an association that is based on the interests of its members, individuals or institutions. It is not created by a government, but it may work cooperatively with the government. Such organizations serve a public purpose, not a private benefit. Examples of NGOs include faith-based charity organizations and the American Red Cross. NGOs, including voluntary and faith-based groups, provide relief services to sustain life, reduce physical and emotional distress, and promote the recovery of disaster victims. 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 (Source: FEMA).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Succession** – A “formal, sequential assumption of a position’s authorities and responsibilities, to the extent not otherwise limited by law, by the holder of another specified position as identified in statute, executive order, or other presidential directive, or by relevant department or agency policy,



order, or regulation if there is no applicable executive order, other presidential directive, or statute in the event of a vacancy in office or a position holder dies, resigns, or is otherwise unable to perform the functions and duties of that pertinent position” (Source: PPD-40, *National Continuity Policy*).

**Telework** – A flexible work arrangement under which an employee performs the duties and responsibilities of the position from an approved worksite other than the location where the work activities of the employee’s position of record are based (Source: FEMA).

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

**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 (Source: FEMA).

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

This page intentionally left blank

## Annex 3: Acronyms

<b>CAG</b>	Continuity Advisory Group
<b>CBRNE</b>	Chemical, Biological, Radiological, Nuclear and Explosive
<b>C.F.R.</b>	Code of Federal Regulations
<b>CISA</b>	Cybersecurity and Infrastructure Security Agency
<b>COG</b>	Continuity of Government
<b>D/A</b>	Department and Agency
<b>DERG</b>	Devolution Emergency Response Group
<b>DHS</b>	Department of Homeland Security
<b>ECG</b>	Enduring Constitutional Government
<b>EO</b>	Executive Order
<b>EOP</b>	Executive Office of the President
<b>ERG</b>	Emergency Relocation Group
<b>FCD</b>	Federal Continuity Directive
<b>FEMA</b>	Federal Emergency Management Agency
<b>FMRS</b>	Federal Mission Resilience Strategy
<b>HVA</b>	High Value Assets
<b>ICWG</b>	Interagency Continuity Working Group
<b>IT</b>	Information Technology
<b>MEF</b>	Mission Essential Function
<b>NARA</b>	National Archives and Records Administration
<b>NCR</b>	National Capital Region
<b>NEF</b>	National Essential Function

<b>NGO</b>	Nongovernmental Organization
<b>NIST</b>	National Institute of Standards and Technology
<b>ONCP</b>	Office of National Continuity Programs
<b>PACE</b>	Primary, Alternate, Contingency, Emergency
<b>PMEF</b>	Primary Mission Essential Function
<b>PPBE</b>	Planning, Programming, Budgeting and Execution
<b>PPD</b>	Presidential Policy Directive
<b>SLTT</b>	State, Local, Tribal and Territorial
<b>U.S.</b>	United States
<b>U.S.C.</b>	United States Code
<b>USPS</b>	United States Postal Service
<b>WMD</b>	Weapon of Mass Destruction