Federal Continuity Directive

Federal Executive Branch Essential Functions Risk Identification and Management

FEMA Office of National Continuity Programs

August 2024

This page intentionally left blank

Table of Contents

1. Applicability and Scope

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

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

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

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

1.1. Supersession

This FCD rescinds and supersedes FCD-2, *Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process*, June 2017.

2. Handling

2.1. Distribution

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

2.2. Operations Security

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

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

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

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

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

2.3. Point of Contact

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

3. Executive Summary

This FCD, *Federal Executive Branch Essential Functions Risk Identification and Management*, directs the implementation of a risk-based approach to continuity of government (COG) and outlines key concepts and methodologies for threat and hazard impact mitigation. This includes processes for identifying essential functions and supporting activities; accounting for the resources and processes needed to perform them; identifying vulnerabilities and resultant essential function risks; and implementing risk mitigation strategies.

Each Federal Executive Branch organization must identify its essential functions and analyze the resources and processes needed to accomplish them. The collective functions of Federal Executive Branch organizations are called Government Functions. Essential functions are subsets of these Government Functions that are categorized as MEFs, Primary Mission Essential Functions (PMEFs), and National Essential Functions (NEFs).

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

After MEFs are identified and validated by the organization's leadership, a business process analysis (BPA) of the MEFs is conducted. A BPA is a systematic method of examining, identifying, and mapping the processes, continuity planning factors (Staff and Organization, Equipment and Systems, Information and Data, and Sites), and other resources (including budget) needed to perform a MEF. Essential supporting activities (ESAs), which are select mission support activities that enable or facilitate the performance of its essential functions, are also identified during the BPA.

The organization then conducts a business impact analysis (BIA) to assess the risk to each of its essential functions. The BIA provides a method of identifying threats and hazards that may impact the performance of these functions, along with problem areas such as resource gaps, process weaknesses, consolidated points of failure, and other vulnerabilities. This analysis enables the organization to identify continuity options (such as distribution, devolution, relocation, and hardening) to close gaps and address vulnerabilities and potential consequences for the performance of its essential functions.

Completing these processes allows the organization to prioritize investments that improve its own essential function resilience, which in turn contributes to National Continuity, including Federal Mission Resilience, across the Federal Executive Branch.

4. Background

This FCD is one of a series of new and revised FCDs that provide direction and guidance for the Federal Executive Branch. It builds on the organizing structure set forth in *FCD: Continuity Planning Framework for the Federal Executive Branch*, illustrated in Figure 1 and used throughout the FCDs, representing the progression of the risk management process toward achieving essential function resilience.

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

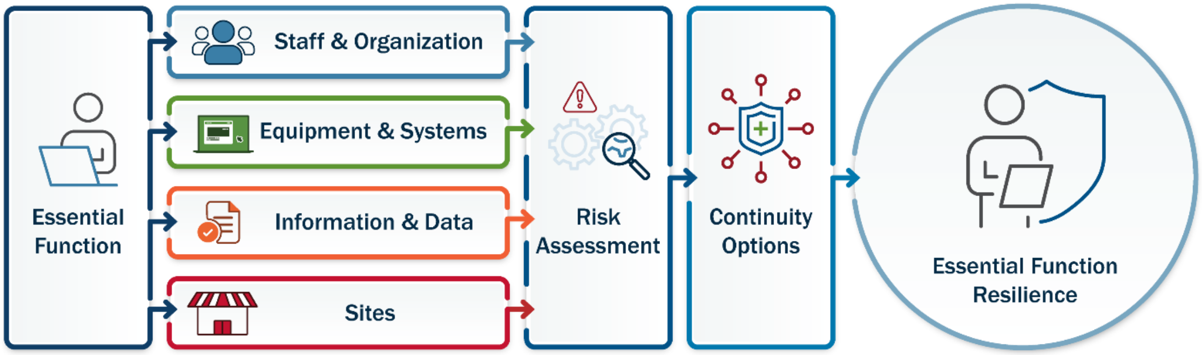

Figure 1: Continuity Planning Framework

Risk management is a responsibility shared by the organization's Continuity Coordinator, Mission Owners, and key enablers (e.g., Chief Information Officers [CIOs] and Chief Security Officers) and is reflected in its continuity program. The Continuity Coordinator ensures that risk to all of the organization's essential functions is integrated into its enterprise risk management, strategic planning, and budgeting processes. Mission Owners assess and address vulnerabilities specific to their operations. The organization's continuity program, in close partnership with Mission Owners and key enablers, addresses ways to mitigate organization-wide vulnerabilities through continuity planning, procurement, and other program activities.

Continuity risk management processes should integrate with and complement the organization's enterprise risk management practices as presented in the Office of Management and Budget (OMB) Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal*

Control.[2] Continuity planning and budgeting should inform broader agency planning and resource allocation decisions consistent with OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*.[3] The organization's continuity program should build on its existing emergency management activities and encompass its most vital operations.

Effective continuity risk management requires increased Deputy Secretary-level attention and engagement to provide Continuity Coordinators with department-wide access to essential function leadership and organizational leadership priorities. Assessing and managing risk to essential functions is a whole-of-organization endeavor, requiring the involvement of leaders, Mission Owners, staff, and stakeholders from across the organization. It cannot be the sole responsibility of a single component within the organization.

4.1. Purpose

This FCD outlines methodologies and concepts for Federal Executive Branch organizations to accelerate their resilience against all threats and hazards, including through a structure of distributed risk and capabilities. The directive details the process for identifying essential functions, understanding the resources and processes needed to perform them, identifying risk to these functions, and ultimately deciding how best to mitigate that risk.

4.2. Policy

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

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

Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities*, directs the head of each organization to ensure the continuity of essential functions in any national security emergency. It also designates the FEMA Administrator as an advisor to the National Security Council on issues of national security emergency preparedness, including COG, and is charged with coordinating the development and implementation of plans for the operation and continuity of

[2] Circular No. A-123 (whitehouse.gov)

[3] Circular No. A-11 (whitehouse.gov)

essential domestic emergency functions of the federal government during national security emergencies.

5. Essential Functions

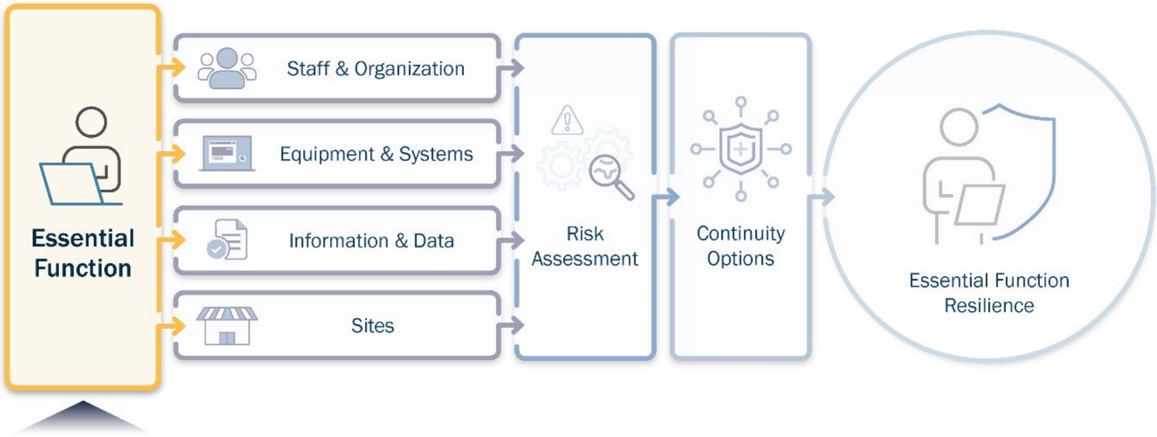

Figure 2: Continuity Planning Framework – Essential Functions

5.1. Overview

The organization must begin by determining what its essential functions are. This section provides guidance on how to identify essential functions and other activities required to accomplish their statutory and foundational missions. Each type of function and activity falls into one or more of the following categories.

Government Functions are the collective functions of Federal Executive Branch organizations as defined by statute, regulation, presidential directive, or other legal authority. (The functions of the legislative and judicial branches are also Government Functions but fall outside the scope of this directive.)

Essential functions are subsets of Government Functions that are categorized as MEFs, PMEFs, and NEFs. Although an essential function does not necessarily need to be performed continuously, it must be performed when required, regardless of conditions or circumstances.

Mission Essential Functions, or MEFs, are unique Government Functions that are directly related to accomplishing an enduring, organizational-level mission (or missions) as set forth in the organization's statutory or executive charter. Because MEFs directly accomplish a specific mission, they tend to be unique to the organization performing them. MEFs consist of one or more Government Functions accomplished by one or more components within the organization.

Primary Mission Essential Functions, or PMEFs, are an elevated subset of the organization's MEFs that, in addition to directly accomplishing the organization's mission, must be continuously performed to support or implement the uninterrupted performance of NEFs (detailed below). Not all organizations have PMEFs.

A PMEF may consist of a single MEF or multiple MEFs, as shown in Figure 3. This determination is made in the IAB process, which is detailed in the Candidate PMEF Submission section of this FCD. Organizations should be aware that a PMEF composed of multiple MEFs may have a different risk profile than its constituent MEFs. In these cases, the "bundled" PMEF must undergo a risk assessment in addition to the risk assessments done for the individual MEFs comprising it.

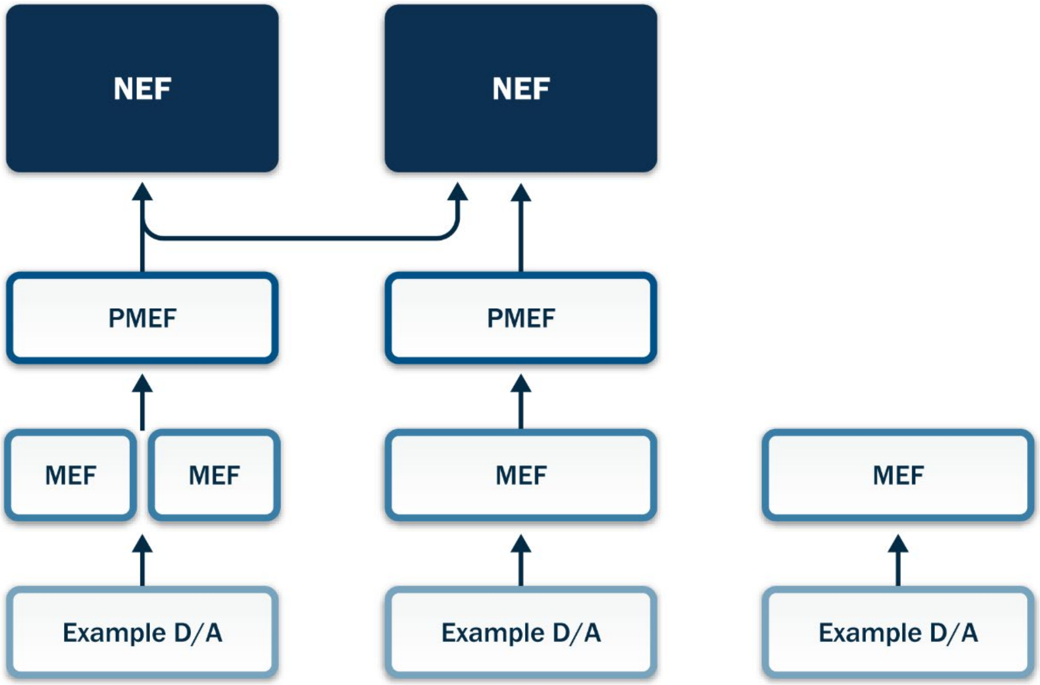

Figure 3: MEF, PMEF, and NEF Alignment

The eight **National Essential Functions, or NEFs,** are the foundation of all continuity programs and capabilities. They represent the overarching responsibilities of the federal government to lead and sustain the Nation. They are therefore the primary focus of federal government leadership before, during, and after a catastrophic emergency.

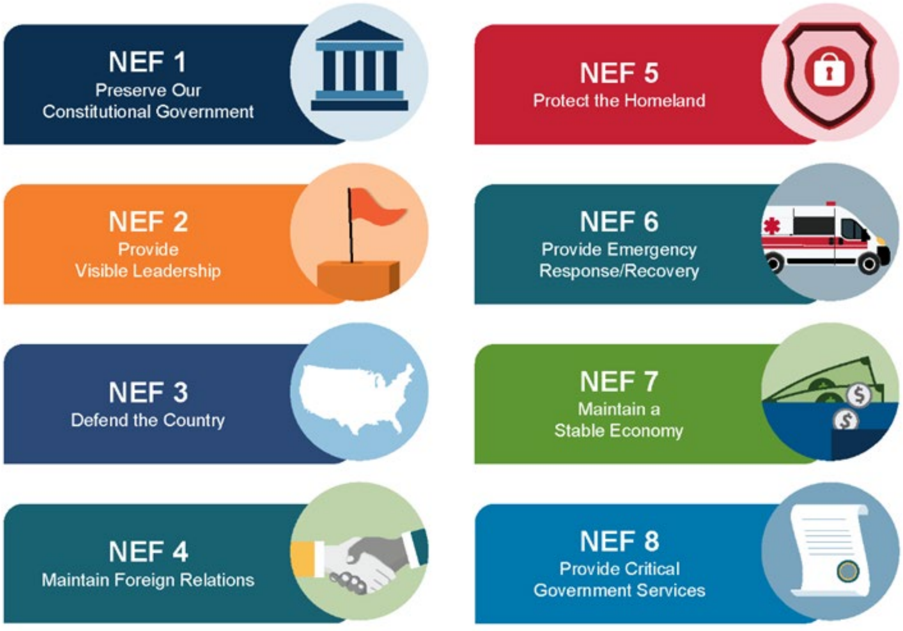
NEF 1
Preserve Our Constitutional Government
NEF 2
Provide Visible Leadership
NEF 3
Defend the Country
NEF 4
Maintain Foreign Relations
NEF 5
Protect the Homeland
NEF 6
Provide Emergency Response/Recovery
NEF 7
Maintain a Stable Economy
NEF 8
Provide Critical Government Services

Figure 4: National Essential Functions

National Essential Functions

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.

Essential Supporting Activities, or ESAs, are select mission support activities performed by the organization that enable or facilitate the performance of its essential functions (e.g., providing a secure workplace, ensuring computer systems are operating). ESAs are not categorized as essential functions, but the essential functions they support could not be performed without the ESA. ESAs consist of one or more support activities accomplished by one or more components within the organization. Organizations may choose to categorize some ESAs as internal dependencies but must ensure this distinction does not obscure the fact that MEF resilience is a whole-of-organization responsibility.

External dependencies are vital activities and services performed for the organization by partners outside the legal or statutory authority of the organization. Although organizations have less control over external partners than over their own plans and operations, they must consider the resilience of these partners when determining the resilience of their own essential functions. This can be done by asking if the partner has a continuity of operations plan, a business continuity plan, and/or an information technology (IT) disaster recovery plan in the case of private-sector entities.

5.2. Essential Function Identification and Validation Process

Essential function identification and validation require an in-depth understanding of the organization, its Government Functions, its foundational mission(s), and how those missions are accomplished. Organizational leadership, Mission Owners/operators, and legal counsel must work together to ensure that they explore all relevant considerations.

Annex A Resources

Organizations may use the Organizational Functions Worksheet (Annex A, Form 1) to assist with identifying and recording essential functions or develop worksheets of their own.

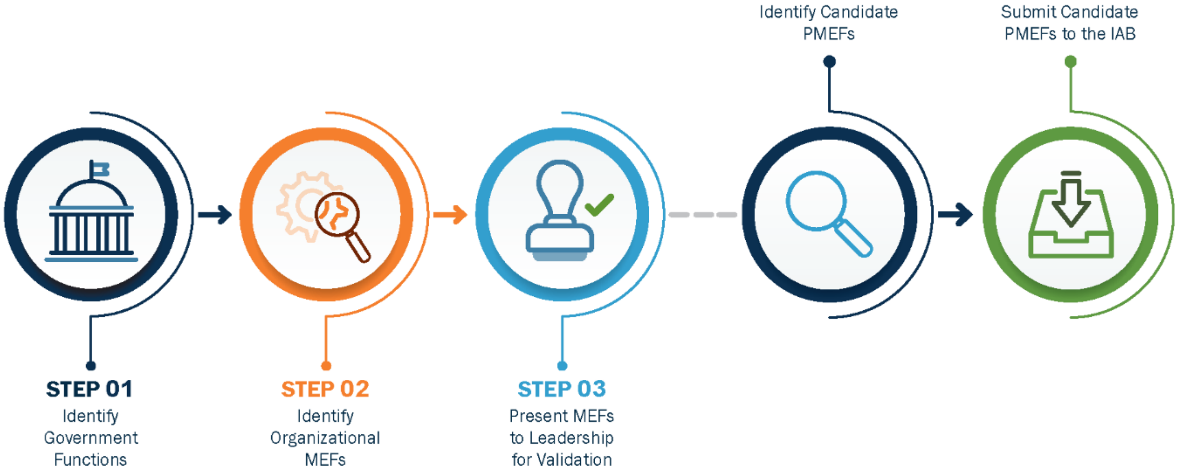
Identify Candidate PMEFs
Submit Candidate PMEFs to the IAB
STEP 01
Identify Government Functions
STEP 02
Identify Organizational MEFs
STEP 03
Present MEFs to Leadership for Validation

Figure 5: MEF and PMEF Identification and Validation Process

5.2.1. IDENTIFYING AND VALIDATING MISSION ESSENTIAL FUNCTIONS

Step 1: Identify Government Functions.

In this step, the organization identifies and lists all major Government Functions that directly support the performance of its enduring, organizational-level mission(s). As part of this step, the organization may review and validate existing lists of Government Functions, as appropriate.

The list of Government Functions must include:

- A description of each function in basic terms;
- The requirement to perform each function, listing the applicable statute, regulation, presidential directive, or other legal authority; and
- The products or services delivered (outputs) or actions each function accomplishes.

Step 2: Identify Organizational MEFs.

After identifying and listing all major Government Functions that support the performance of its enduring, organizational-level mission(s), the organization must identify which are essential and which are nonessential.

Organizations must assign **maximum tolerable downtime (MTD)** to each essential function and ESA. MTD is the longest amount of time an essential function may be disrupted before it results in unacceptable degradation of the mission it accomplishes. It is informed by the MTDs for the planning factors. Specific to the Information and Data planning factor, a **recovery time objective (RTO)** is the maximum amount of time that information and data can be unavailable before it negatively impacts its function. A **recovery point objective (RPO)** refers to the point in time, prior to a disruption, at which data can be recovered.

Essential functions cannot be deferred past MTD without causing serious degradation or failure of the mission, even during emergencies. Functions that can be deferred until after an emergency are identified as nonessential.

MEFs are the Government Functions directly related to accomplishing the organization's foundational missions that cannot be deferred past MTD without causing serious degradation or failure of those missions, even during an emergency that disrupts normal operations.

Example: MEF

FEMA MEF 3: Lead and coordinate national emergency recovery efforts following a disaster to ensure that appropriate, timely federal assistance is delivered to the impacted population and region to minimize disruption of services and facilitate a return to normalcy.

When identifying MEFs, organizations should:

- Concurrently review existing MEFs and make necessary updates or validate information, as appropriate.
- Review the functions performed both at HQ and at other sites where the organization's mission is executed. Although command and control generally occurs at HQ sites, the actual performance of most essential functions occurs elsewhere.
- Identify and leverage the expertise of the Mission Owner/operator of each MEF in this process to ensure that complete, accurate, and up-to-date information is obtained.

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.

Step 3: Present MEFs to Leadership for Validation.

After completing the previous steps, the organization should then present its updated, validated, or new MEFs to leadership for initial review and concurrence. Obtaining concurrence or approval of MEFs at this point allows the organization to begin conducting an efficient, effective, and targeted BPA and BIA of the identified MEFs.

Annex A Resources

Organizations are encouraged to use the Mission Essential Function Data Sheet (Annex A, Form 2) to record information about their MEFs.

5.2.2. IDENTIFYING AND VALIDATING PRIMARY MISSION ESSENTIAL FUNCTIONS

Once organizations have identified and validated their MEFs, they must analyze these functions to determine if (a) any should be considered a candidate PMEF or (b) a consolidated group of focused MEFs represent a broader function that could be considered a candidate PMEF. Either of these instances can occur when a single MEF or a consolidated group of focused MEFs support the continual performance of one or more NEFs. During the analysis of candidate PMEFs, organizations must also review existing PMEFs to identify any changes within the PMEF resulting from evolving performance requirements.

Organizations must review their MEFs and PMEFs every two years to determine if a candidate PMEF continues to support the NEFs.

Candidate PMEF Identification and Analysis

Organizations must determine if a MEF, an existing PMEF as written, or a change to a PMEF may be identified as a candidate PMEF.

1. Identify the requirement to perform the MEF or candidate PMEF by listing the statute, regulation, presidential directive, or other legal authority.
2. Determine whether the MEF or candidate PMEF function must be continuously performed to support or implement the uninterrupted performance of NEFs.

Annex A Resources

Organizations must document the candidate PMEF by completing the Candidate Primary Mission Essential Function Worksheet (Annex A, Form 5).

Candidate PMEF Submission

FEMA manages and coordinates the PMEF review and validation cycle to review and recommend candidate PMEFs prior to submission to the National Continuity Coordinator (NCC) for final approval (validation). An objective IAB process is used to ensure that a consistent validation standard is applied across the Federal Executive Branch. FEMA manages, coordinates, and serves as the executive agent of the IAB.

The following documents must be included in candidate PMEF submission packages to FEMA ONCP in support of IAB review:

- **Agency Memorandum:** The organization’s Continuity Coordinator submits a memorandum to the IAB that proposes a revised, rescinded, consolidated, or new candidate PMEF. The memorandum must include contact information for both the Continuity Coordinator and Continuity Program Manager for IAB coordination.
- **Candidate PMEF Data Worksheet:** Information documented in the MEF identification, BPA, and BIA processes must be used to complete the worksheet. The worksheet includes a brief statement identifying the candidate PMEF, a narrative description, an impact statement concerning PMEF failure, identification of the supported NEF, MTD, dependencies and interdependencies, and a point of contact.
- **BPA and BIA Documentation:** Organizations must have current BPA and BIA reports and other appropriate documentation supporting the candidate PMEF available for review during the IAB process.

Interagency Board Process

FEMA plans and coordinates the IAB joint review and validation recommendation process for submitted candidate PMEFs. Organizations’ continuity and functional subject-matter experts evaluate the relationship of each PMEF to the NEFs.

FEMA ONCP will consolidate the IAB recommendations and submit the recommended PMEFs and supporting documentation through the FEMA Administrator to the NCC for review and approval.

6. Essential Function Business Process Analysis

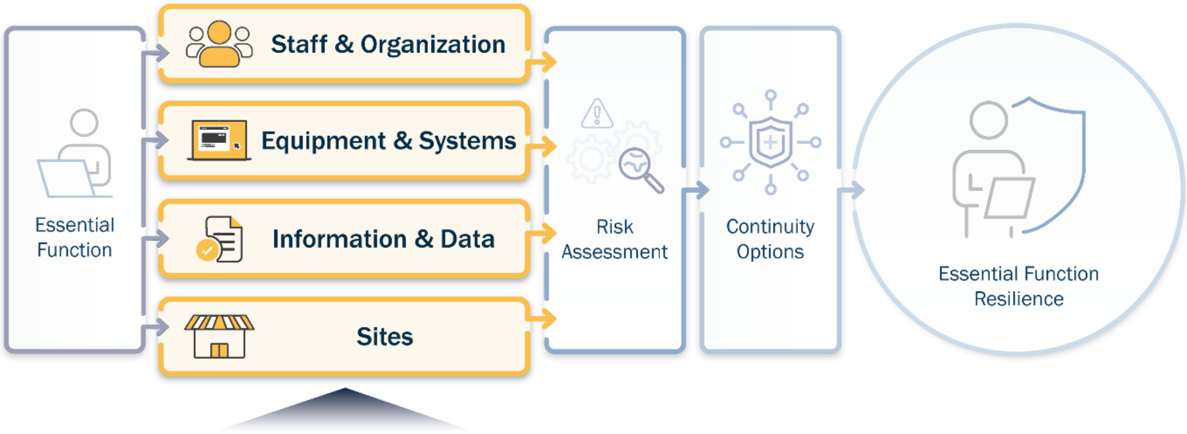

Figure 6: Continuity Planning Framework – BPA

6.1. Overview

After leadership has validated the MEFs, organizations must conduct a BPA of these functions. A BPA is a systematic method of examining, identifying, and mapping the tasks, continuity planning factors (Staff and Organization, Equipment and Systems, Information and Data, and Sites), ESAs, external dependencies, and other resources (including budget) needed to perform a MEF.

OPSEC Note: Classified Information and the BPA

Prior to compiling information for a BPA, organizations should review applicable security classification guides—including those of FEMA, individual D/As, MEF operations programs, and external partners—to ensure proper classification, handling, and storage of all products developed for the BPA. Some information and data may need to be reclassified when compiled with other information and data. Any questions should be elevated to leadership and organizational security, as appropriate.

6.2. Conducting the Business Process Analysis

The Mission Owner of each MEF has the primary responsibility for conducting the BPA in coordination with staff performing the function and other key partners; each organization must determine who should be involved. This ensures that every relevant consideration is made when documenting how the MEF is performed. Continuity program personnel coordinate this and other continuity requirements.

Annex A Resources

Organizations are encouraged to use the Mission Essential Function Data Sheet (Annex A, Form 2) to record information about their MEFs.

Organizations may use the Business Process Analysis Data Sheet to record information about MEFs (Annex A, Form 3) during this process or may develop data sheets of their own.

In compiling the BPA, organizations should consider:

- Generic operational requirements of the function (e.g., “approximately 300 square feet of secure, accessible, co-located workspace with at least six individual workstations”);
- How those requirements are or could be met during normal operations with proactive continuity options, such as distributed or hardened continuity planning factors; and
- How those requirements are or could be met with reactive continuity options, such as relocated or devolved continuity planning factors.

Information in the BPA does not need to be as specific as that in existing continuity implementation plans, standard operating procedures, operation plans, and so forth, but it should cite that information and where/how it may be accessed.

The BPA is presented here as sequential steps, but organizations may merge, rearrange, and add to these steps, provided that all necessary factors are analyzed and documented. If continuity planning factors (Staff and Organization, Equipment and Systems, Information and Data, and Sites) are shared among multiple components within the organization, it is vital that joint planning sessions are conducted to address and mitigate shared risk.

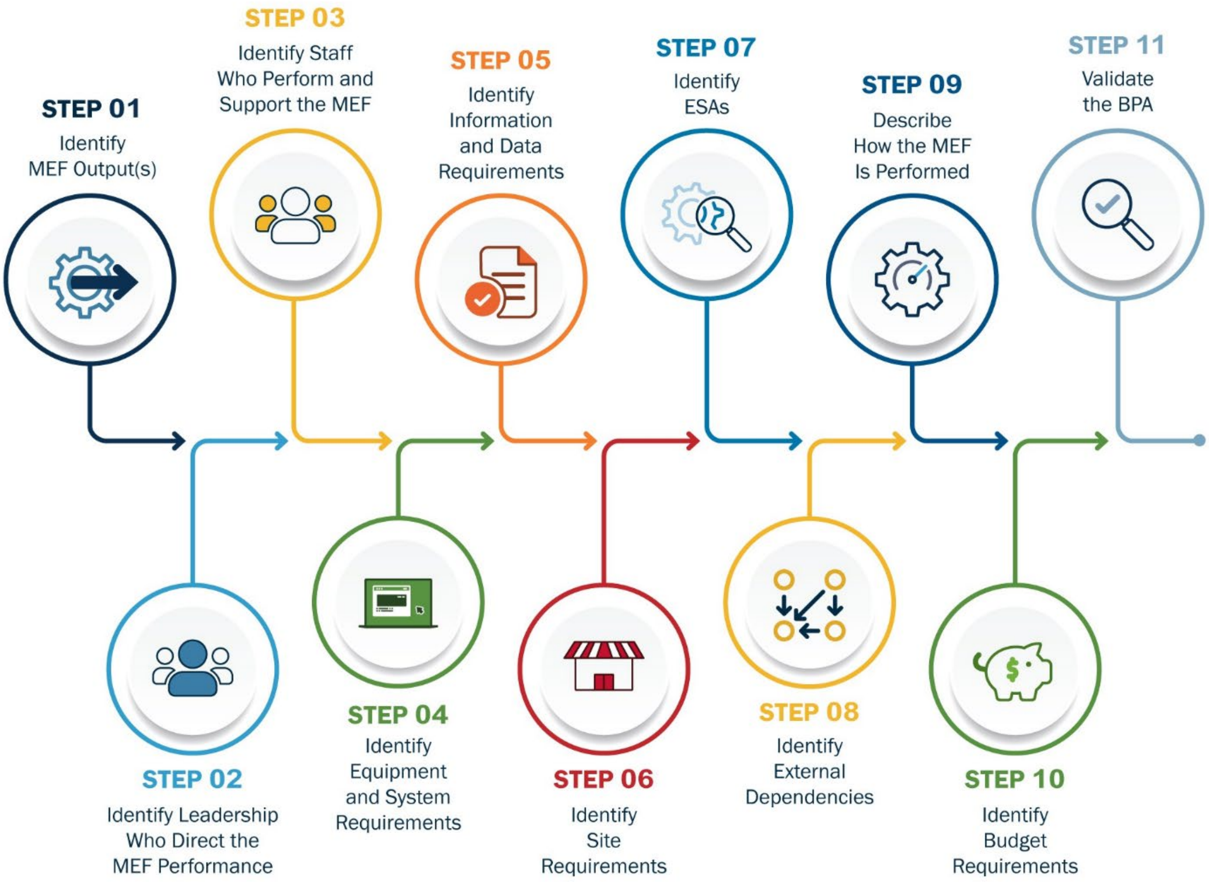
STEP 01
Identify MEF Output(s)
STEP 02
Identify Leadership Who Direct the MEF Performance
STEP 03
Identify Staff Who Perform and Support the MEF
STEP 04
Identify Equipment and System Requirements
STEP 05
Identify Information and Data Requirements
STEP 06
Identify Site Requirements
STEP 07
Identify ESAs
STEP 08
Identify External Dependencies
STEP 09
Describe How the MEF Is Performed
STEP 10
Identify Budget Requirements
STEP 11
Validate the BPA

Figure 7: BPA Process

Step 1: Identify MEF Output(s).

In this step of the BPA, organizations identify products, services, and information (i.e., deliverables or outputs) that result from the performance of the MEF and annotate them on the BPA worksheet. The description must include appropriate metrics that identify specific performance measures and standards, such as timeframes for when products and services are needed and whether the output may be altered during an emergency without compromising the organization’s mission. These MEF output metrics will inform the BIA.

Example: MEF Output

A report that supports major disaster declaration decisions is given to the President of the United States within two hours of a disaster.

Staff & Organization

Step 2: Identify Leadership Who Direct the MEF’s Performance.

This step identifies the organizational leadership positions required to provide command and control, make decisions, and perform other key actions necessary to ensure the continuity of the MEF and/or any of its vital constituent tasks. At a minimum, the description must include the location of appropriate senior leadership positions and specify if their actions can be performed remotely or if they are needed at a certain facility.

Once leadership requirements have been identified, descriptions must be annotated on the BPA worksheet and should include the following, as applicable:

- The position title;
- Site (location[s] from which essential functions are performed);
- Communication requirements;
- MTD; and
- Clarifying notes, as required.

Example: Leadership Description

Deputy Assistant Secretary at alternate site #3 with Category II minimum communications equipment within four hours.

A description must be provided for each leadership position required to ensure the continuity of a MEF. ESA and external dependency requirements are recorded in later steps.

Step 3: Identify Staff Who Perform and Support the MEF.

In this step, organizations identify and describe the staff required to ensure the continuity of the MEF and/or any of its vital constituent tasks. Descriptions must include the number of staff required and specify the appropriate knowledge, skills, abilities, expertise, experience, certifications, licenses, and clearances or permissions needed for each position.

Once staff requirements have been identified, descriptions must be annotated on the BPA worksheet and should include the following, as applicable:

- Quantity of staff needed by position;
- The position title;
- Clearance level required;
- Special knowledge, skills, or abilities;
- Continuity duty site (site from which continuity operations are performed);

- RTO; and
- Clarifying notes, as required.

Example: Staff Description

Four licensed civil engineers with secret clearance experienced in road and bridge safety and inspection requirements at the alternate operating facility within eight hours.

A description must be provided for each staff position required to ensure the continuity of the MEF. ESA and external dependency requirements are recorded in later steps.

Equipment & Systems

Step 4: Identify Equipment and System Requirements.

In this step, organizations identify information and communications technology (ICT) systems and other equipment required to ensure the continuity of the MEF and/or any of its vital constituent tasks. This requires coordination among Mission Owners/operators, the Office of the CIO, the High Value Asset Point of Contact, and any other offices charged with categorizing equipment and systems as mission essential.

A **high value asset (HVA)** is "information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have a serious impact on the organization's ability to perform its mission or conduct business."[4]

Organizations must:

- Appropriately allocate agency resources for HVAs to ensure the effective protection of these systems;
- Ensure the mission critical systems that support the performance of essential functions are listed as HVAs and business essential systems; and
- Determine if additional resources are needed to protect them.

This is achieved through collaboration among organization CIOs, Chief Information Security Officers (CISOs), Chief Financial Officers (CFOs), Senior Agency Officials for Privacy (SAOPs), and other roles—in coordination with OMB and DHS.

[4] CISA Insights - Cyber: Secure High Value Assets (HVAs)

Once equipment and system requirements have been identified, descriptions must be annotated on the BPA worksheet and should include the following, as applicable:

- System owner;
- Name of the system;
- System classification requirement (e.g., U, S, TS, SCI);[5]
- Hosting/housing site;
- MTD; and
- Clarifying notes, as required.

The Cybersecurity and Infrastructure Security Agency's (CISA) Shields Up campaign provides recommendations, products, and resources to increase organizational vigilance and keep stakeholders informed about cybersecurity threats and mitigation techniques.[6] The complementary Shields Ready campaign provides guidance on identifying critical assets, mapping dependencies, developing plans and exercise capabilities, and implementing program evaluation and improvement activities to reinforce readiness.[7]

A description must be provided for all equipment and systems required to ensure the continuity of the MEF. ESA and external dependency requirements are recorded in later steps.

Minimum Communications Requirements

Category I, II, and III executive D/A HQ and alternate sites must meet minimum communications requirements detailed in Office of Science and Technology Policy (OSTP)/OMB Directive D-16-1, *Minimum Requirements for Federal Executive Branch Continuity Communications Capabilities*, as amended, and its annexes.

Information & Data

Step 5: Identify Information and Data Requirements.

In this step, organizations identify the information and data required to ensure the continuity of the MEF and/or any of its vital constituent tasks. The Mission Owners/operators receiving and using specific information and data to perform the MEF must be consulted to ensure a comprehensive list

[5] U: Unclassified; S: Secret; TS: Top Secret; SCI: Sensitive Compartmentalized Information.

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

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

is created and establish the minimally acceptable amount of data loss through the RPO setting as well as the minimally acceptable period without access to the data through the RTO.

Once information and data requirements have been identified, descriptions must be annotated on the BPA worksheet and should include the following, as applicable:

- The document/form name, or a description of the information or data;
- Where the information will come from or where it can be accessed;
- The classification level or other unique access requirements (e.g., U, S, TS, SCI);
- RPO and RTO; and
- Clarifying notes, as required.

Example: Information and Data Description

FEMA Headquarters Continuity Plan (FI-302-095-1b-1), hard copy in alternate site safe and electronic copy on FEMA continuity server, U//FOUO [For Official Use Only], immediately available.

A description must be provided for all specific information and data required to ensure the continuity of the MEF. ESA and external dependency requirements are recorded in later steps.

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)."[8] 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 emergency.[9]

Sites

Step 6: Identify Site Requirements.

In this step, organizations identify each site required to ensure the continuity of the MEF and/or any of its vital constituent tasks. This includes MEF performance and command and control.

[8] Essential Records Information | National Archives

[9] Essential Records Guide (archives.gov)

Organizations must identify the requirements for minimum space, configuration, security, safety, support services (e.g., lodging, food services, medical support), and storage appropriate for their operations.

As with every other planning factor, Mission Owner/operator input in coordination with support staff and other relevant stakeholders is needed to ensure all vital information is captured and all relevant factors are accounted for.

Following a disruption, organizations must be able to perform all their essential functions as soon as possible, but not later than 12 hours after continuity plan activation, and sustain them for a minimum of 30 days or until normal operations are resumed. The BPA should reflect this capability.

Telework and remote work can provide additional flexibility in situations where commercial infrastructure is still functional. Organizations may choose to leverage them to sustain their essential functions, but they must maintain a site that meets *National Continuity Policy* requirements. Category I, II, and III executive D/As must also meet OSTP/OMB D-16-1 communications requirements.

Alternate Site Resilience Resources

Resources such as CISA's *Resilient Power Best Practices for Critical Facilities and Sites* and the Interagency Security Committee's (ISC) *The Risk Management Process* are useful tools to help organizations assess and ensure site resilience.[10]

Once site requirements have been identified, descriptions must be annotated on the BPA worksheet and should include the following, as applicable:

- Required site type and size (e.g., general office space of 40,000 square feet);
- Intended continuity use (e.g., hardened/distributed primary, relocation, devolution);
- Classified space requirement (e.g., U, S, TS, SCI);
- Data network access requirement (e.g., U, S, TS, SCI);
- Support service requirements (e.g., lodging, food services, security, medical support);
- MTD; and
- Clarifying notes, as required.

[10] See Resilient Power Best Practices for Critical Facilities and Sites | CISA. Also, *The Risk Management Process: An Interagency Security Committee Standard* establishes a single, formalized process for determining federal site security requirements. It helps organizations understand the potential impacts of threats and hazards, develop risk management strategies, and establish a culture of risk awareness and resilience.

Note: Once the site has been procured, the actual site specifications, including the site name and location, should also be recorded.

Example: Site Description

Operations center of 2,500 square feet, alternate site (relocation), 12 UNCLASSIFIED and six SECRET workspace and data networks, 24/7 secure access with lodging for 12 people, basic utilities, food, water, and backup power, provisioned for 30-day continuous use by 12 personnel, fully operational within two hours.

A description must be provided for all sites required to ensure the continuity of the MEF. ESA and external dependency requirements are recorded in later steps.

Step 7: Identify Essential Supporting Activities.

In this step, organizations identify the vital mission support activities that indirectly accomplish the MEF by enabling or facilitating its performance (e.g., providing a secure workplace, ensuring computer systems are operating). ESAs are only those activities that would result in severe degradation or failure of an essential function if they were not available. Unlike external dependencies, ESAs are performed internally by the organization performing the MEF.

Once ESAs have been identified, descriptions must be annotated on the BPA worksheet and should include the following, as applicable:

- ESA component name;
- Concise statement of the ESA, including who, what, when, where, why, and how, as appropriate;
- MTD;
- ESA point of contact and contact information; and
- Clarifying notes, as required.

A description must be provided for all ESAs vital to the continuity of the MEF. External dependency requirements are recorded in the following step.

Note: The component performing the ESA must be made aware that its activity is necessary for the organization's performance of a MEF.

Step 8: Identify External Dependencies.

In most cases, organizations rely on external partners and infrastructure to meet at least some of their mission requirements. This step focuses on identifying those external partners and infrastructure and what they provide to the organization. The list should include other organizations, SLTT authorities, critical infrastructure owners and operators, nongovernmental organizations (NGOs), private-sector organizations, supply chains, and others as appropriate.

Supply chains can be challenging to account for, but they are often critical to the performance of an essential function. Many resources are available to help organizations account for this often-vital component of essential function performance.[11]

Once external dependencies have been identified, descriptions must be annotated on the BPA worksheet and should include the following, as applicable:

- Supporting partner name;
- Concise statement of the dependency, including who, what, when, where, why, and how, as appropriate;
- MTD;
- Partner point of contact and contact information; and
- Clarifying notes, including relevant support memoranda or other agreements, as required.

A description must be provided for all external dependencies vital to the continuity of the MEF.

Note: Partner organizations must be made aware that their products or services are necessary for the organization's performance of a MEF. If the organization knows that an interdependency (mutual dependency) exists with an external organization, it is encouraged to list this interdependency in the BPA.

Step 9: Describe How the MEF Is Performed.

In this step, organizations develop a narrative description of performing the MEF to produce the outputs discussed in Step 1 and annotate it on the BPA worksheet. Organizations will develop appropriate diagrams or other informational aids to support the narrative description. Documenting the process aids in identifying and validating other BPA information and limits the omission of relevant details.

Organizations must identify when in the process each input is needed and when each output must be produced, because some may be initially required and others may be needed later. Organizations must also identify if some level of MEF degradation is tolerable (e.g., outputs may be reduced to some degree without causing mission failure). This timeline will inform MTD allowances. A description must be provided for each MEF.

[11] Resources include CISA's *Vendor Supply Chain Risk Management (SCRM) Template*, the National Institute of Standards and Technology's (NIST) *Key Practices in Cyber Supply Chain Risk Management*, and the National Counterintelligence and Security Center's *Supply Chain Risk Management: Reducing Threats to Key U.S. Supply Chains*, to name just a few.

Step 10: Identify Budget Requirements.

In this step, organizations identify budget requirements to ensure the continuity of the MEF for a minimum of 30 days following a disruption to normal operations. The description must account for funding requirements for all applicable tasks, ESAs, and continuity planning factors, including budgeting related to external dependencies. Budgeting to mitigate risk for the continuity of essential functions and supporting activities should be coordinated with organizational budgeting requirements as presented in OMB Circular No. A-11. A description must be provided for each MEF.

Step 11: Validate the BPA.

In this step, Mission Owners/operators verify that the BPA accurately lists and describes the processes, tasks, ESAs, continuity planning factors, and other resources they require to ensure the continuity of their MEF.

7. Applying Risk Assessment/Business Impact Analysis and Continuity Options to Essential Functions

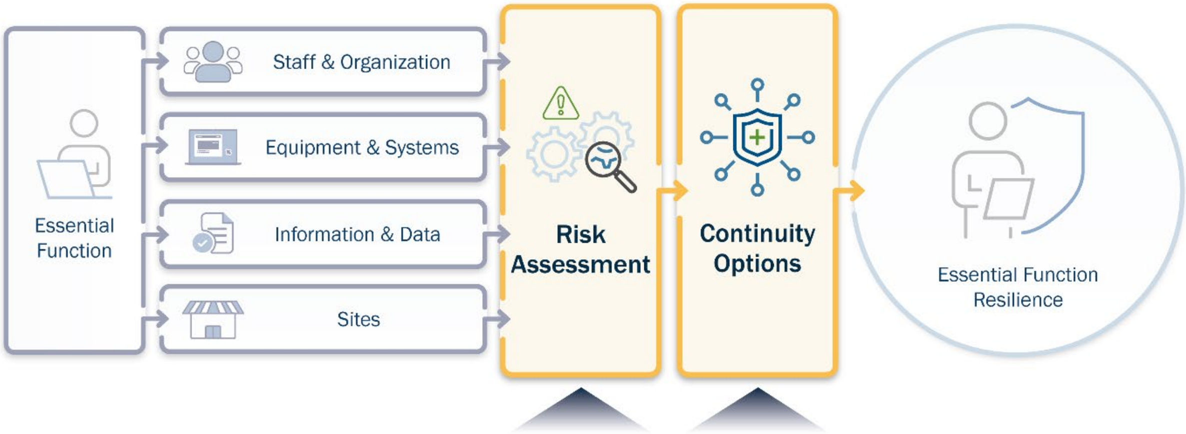

Figure 8: Continuity Planning Framework – Risk Assessment and Continuity Options

7.1. Overview

Organizations must conduct a BIA to assess risk to each of their essential functions. The BIA provides a method of identifying threats and hazards that may impact the performance of these functions, along with problem areas such as resource gaps, process weaknesses, consolidated points of failure, and other vulnerabilities. These and other factors are then used to calculate the risk to essential functions.

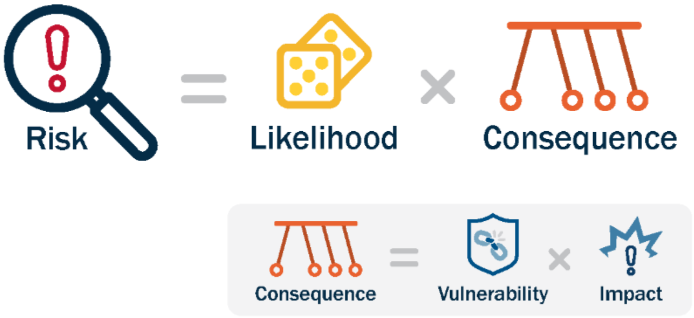

Figure 9: Calculation of Risk from Each Threat/Hazard Event

The results of the BIA inform the adoption of continuity options to mitigate unacceptable risk to essential functions. These include proactive options such as distributing operations and hardening the equipment, systems, and sites used in the performance of essential functions at primary sites.

They also include reactive options such as relocating primary staff or devolving functions to alternate staff. In some instances, the organization may decide to accept the risk.

7.2. Risk Assessment/Business Impact Analysis

The BIA, like the BPA, requires an in-depth understanding of each identified MEF. An effective assessment should inform and be informed by organizational priorities and complement other mission assurance and risk management plans and programs. It should include leadership and Mission Owners/operators most familiar with the essential function. It should also include mission assurance, enterprise risk, and emergency management practitioners familiar with threats, hazards, and risk to the organization. Assessing risk cannot be the sole responsibility of a single component within the organization.

OPSEC Note: Classified Information and the BIA

Prior to compiling information for a BIA, organizations should review applicable security classification guides to ensure proper classification, handling, and storage of all products developed for the BIA. Some information and data may need to be reclassified when compiled with other information and data. Any questions should be elevated to leadership and organizational security, as appropriate.

Organizations should conduct a separate analysis for each MEF and consider critical infrastructure, ESAs, and external dependencies that enable or facilitate the MEF. Organizations may leverage existing processes and internal analyses (e.g., a BIA done as part of the enterprise risk management process) to support this BIA, provided the requirements outlined in the FCDs are met.

Annex A Resources

Organizations may use the Business Impact Analysis/Risk Assessment Worksheet (Annex A, Form 4) to record information about their MEFs during this process or develop worksheets of their own.

Organizations are encouraged to continue using the Mission Essential Function Data Sheet (Annex A, Form 2) to record information about their MEFs.

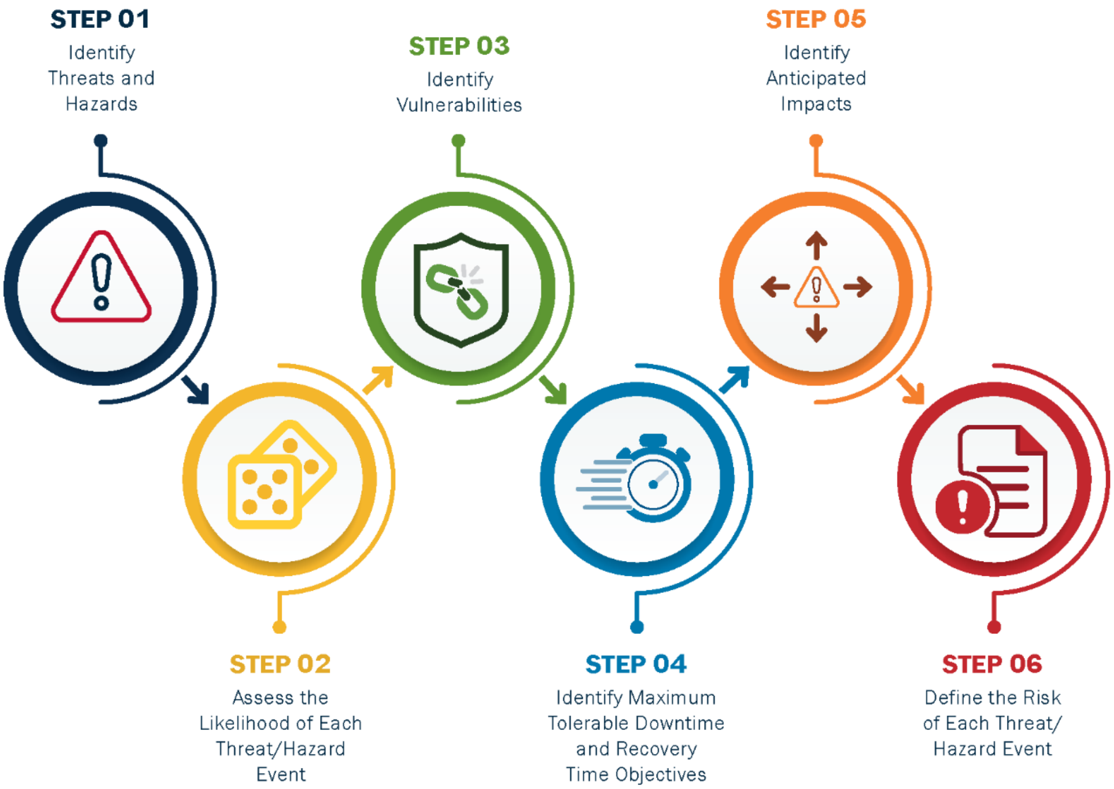
STEP 01
Identify Threats and Hazards
STEP 02
Assess the Likelihood of Each Threat/Hazard Event
STEP 03
Identify Vulnerabilities
STEP 04
Identify Maximum Tolerable Downtime and Recovery Time Objectives
STEP 05
Identify Anticipated Impacts
STEP 06
Define the Risk of Each Threat/ Hazard Event

Figure 10: Risk Assessment/BIA Process

The assessment process entails the following steps that organizations may merge, rearrange, tailor, and supplement to achieve a robust understanding of risk to an essential function.

Step 1: Identify Threats and Hazards.

Organizations must consider existing and emerging threats and hazards. Outpacing a quickly evolving threat landscape requires organizations to maintain an enhanced level of steady-state readiness, with specific attention given to threats and hazards that come without notice and could potentially disrupt the performance of a MEF. This includes specific human-caused threats, natural hazards, technological hazards, and service disruptions. Organizations should consult security, risk, and emergency management practitioners familiar with potential threats and hazards and leverage external resources from the law enforcement and intelligence communities, such as National Intelligence Estimates and the *Annual Threat Assessment of the U.S. Intelligence Community*.[12]

[12] 2024 Annual Threat Assessment of the U.S. Intelligence Community (dni.gov)

Other sources may include, but are not limited to:

- Existing federal and SLTT strategic and operational plans;
- Existing threat or hazard assessments (e.g., the Hazard Identification and Risk Assessment);[13]
- Forecasts or models of future risks due to changing weather and demographic patterns or emerging threats;
- Hazard mitigation plans;
- Intelligence fusion center bulletins and assessments;
- Federal, state, local, regional, tribal, and private-sector Threat and Hazard Identification and Risk Assessments (THIRAs);
- Records from previous incidents, including historical data;
- Homeland security and emergency management laws, policies, and procedures; and
- Private-sector plans and risk assessments, including those for lifeline functions (communications, energy, transportation, and water).

Organizations should annotate the threats and hazards they determine pose unacceptable risk to their essential functions. Some of these threats and hazards will be common and well-understood, but others, such as emerging and future threats and hazards, may be more difficult to identify and predict in terms of likelihood and impact. Based on a combination of research, experience, forecasting, subject-matter expertise, and other available resources, organizations develop a list of specific threats and hazards that have the potential to disrupt the day-to-day performance of their essential functions.

> An essential function performed at distributed sites may incur different risks at the different sites (e.g., one site may be in a region prone to hurricanes and another may be in a region prone to earthquakes). The organization's leadership, Continuity Coordinator, and Mission Owners will determine the extent to which the principles outlined in the FCDs apply to components, regional offices, or field offices.

Step 2: Assess the Likelihood of Each Threat/Hazard Event.

Organizations must assess the likelihood of each threat and hazard during a given period and assign a numerical value to each based on this assessment. Organizations may use whatever methods and analytic standards they think are best. The actual likelihood of most threats and hazards occurring in a given period is low, so organizations may decide that calculating the relative, rather than absolute, likelihood is more useful.

[13] See Hazard Information and Analysis Resources (cisa.gov). The ISC's *The Risk Management Process: An Interagency Security Committee Standard*, Appendix A (The Design-Basis Threat Report), lists minimum considerations for all human-caused and other threats facing federal facilities, while Appendix D (How to Conduct a Facility Security Committee) can be a helpful tool for conducting a BPA and BIA.

Organizations should account for circumstances that might alter the assessment over time, including weather, time of day, and time of year.

Table 1: Likelihood of Each Threat/Hazard Event

Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely
Highly improbable	Improbable (improbably)	Roughly even odds	Probable (probably)	Highly probable
1	2	3	4	5

Step 3: Identify Vulnerabilities.

Vulnerabilities are unmitigated conditions and characteristics that make a continuity planning factor (Staff and Organization, Equipment and Systems, Information and Data, or Sites) more susceptible to a threat or hazard. Organizations should assess and record their levels of vulnerability both descriptively (i.e., written narrative) and numerically (e.g., 1 = highly resilient; 5 = highly vulnerable).

Step 4: Identify the MTD.

In this step, organizations verify the overall MTD for each MEF and for specific tasks, ESAs, and continuity planning factors within the MEF, as determined in the BPA.

An **MTD statement** affirms whether the MEF must be performed continuously or how quickly it must be resumed if disrupted to avoid serious degradation or failure of the mission it supports.

These must be considered when rating impacts in Step 5. A low MTD may increase the likelihood or severity of an impact because a function with little-to-no tolerable downtime may be impacted by short-duration events (e.g., a one-hour power outage) that would not impact a function with a high MTD. Describing the extent of the impact of MEF failure in terms of MTDs supports risk-informed decision-making.

Step 5: Identify Anticipated Impacts.

Organizations must analyze each threat and hazard to determine how likely it is to adversely affect the performance of an essential function. Organizations should assess and record impact levels both descriptively (i.e., written narrative) and numerically (e.g., 1 = almost no chance of failure; 5 = almost certain failure). An example is provided in Table 2.

Table 2: Impacts to the MEF from Each Threat/Hazard Event

Impact	Score	Metrics
Severe	5	The organization is unable to perform operations. The MEF is disrupted and surpasses MTD requirements.

Impact	Score	Metrics
High	4	The organization conducts contingency operations using one or more continuity options. The MEF is disrupted but is resumed within MTD requirements.
Moderate	3	The organization conducts contingency operations using one or more continuity options and continues performing the MEF with little-to-no interruption.
Low	2	The organization conducts slightly altered operations and continues performing the MEF with little interruption.
Very Low	1	The organization conducts normal operations and continues performing the MEF with no interruption.

Organizations should provide a short qualitative statement explaining how a threat or hazard could impact each continuity planning factor and cause MEF degradation or failure. The following are examples of considerations:

- **Potential Failure Due to Staff and Organization Impacts:** (a) Does leadership have capable successors and up-to-date orders of succession with appropriate delegations of authority? (b) How dependent is the task on centralized decision-making versus individual initiative? (c) Do primary and alternate staff have the specific skill sets, expertise, clearances, and required authorities to perform a MEF? (d) Are staff dispersed or consolidated at a single site?
- **Potential Failure Due to Equipment and System Impacts:** (a) Is there pre-identified redundancy in alternate, contingency, and emergency equipment and systems? (b) Are systems maintained, and do they meet minimum ICT security standards? (c) Are distributed equipment and systems interoperable? (d) Can the organization obtain, purchase, and transport replacement equipment and systems during or in the immediate aftermath of an emergency? (e) Do these rely on third-party support that could be impacted in an emergency?
- **Potential Failure Due to Information and Data Impacts:** (a) Do internal and external partners know what information and data the organization requires from them? (b) Is redundant data adequate, accessible, and unlikely to be affected by an event impacting primary information and data? (c) Is data provided, stored, or managed by a third party?
- **Potential Failure Due to Site Impacts:** (a) Is an alternate site sufficiently isolated from the primary site—both physically and in terms of dependencies such as water, wastewater, power, and supply/resupply chains—to avoid being impacted by the same event? (b) Is the site self-sufficient or dependent on the external provision of goods and services like public utilities?

Step 6: Define the Risk of Each Threat/Hazard Event.

The following equation is a simplified example to help conceptualize the factors involved in calculating risk. It shows that the *risk* to the essential function equals the *likelihood* of the event occurring multiplied by the *consequence* of the event (the consequence is the product of the *vulnerability* of the function and the anticipated *impact* of the event). Organizations are encouraged to tailor calculations of risk to suit their own risk management requirements.

Risk = Likelihood × Consequence

(***Consequence*** = *Vulnerability* × *Impact*)

Organizations must conduct a formal BIA review and validation as part of the IAB cycle. They must also update BIAs as needed, at the organization's discretion, considering enhancements to or degradation of MEF resilience and ongoing monitoring of the threat and hazard landscape.

7.3. Risk Mitigation Approaches

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

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

Organizations must mitigate unacceptable risk by adopting and employing one or more continuity options.

7.4. Continuity Options

Using the analysis conducted in the BPA and BIA to understand vulnerabilities in the continuity planning factors (Staff and Organization, Equipment and Systems, Information and Data, and Sites) and overall risk to an essential function, organizations then adopt continuity options to mitigate unacceptable risk. Leadership participation in this process ensures that essential function risk management is appropriately prioritized within broader enterprise risk management processes and practices.

Annex A Resources

Organizations may use the BIA/Risk Mitigation Worksheet (Annex A, Form 4) to record information about which continuity options they select for each MEF during this process or develop worksheets of their own.

Identifying continuity options to mitigate common and well-understood threats and hazards is often easier than doing so for uncommon or emerging threats and hazards. These less common and less understood threats and hazards may be best mitigated by planning for impacts to one or more of the continuity planning factors rather than focusing on a specific threat or hazard. For example, flooding, wildfires, and hazardous material releases have different characteristics (e.g., speed of onset, size of the affected area), but each may prevent the use of a primary site. Devolving a function or relocating continuity team members to an alternate site can mitigate an impact to a primary site, irrespective of the cause of the impact.

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

Organizations may select more than one continuity option to reduce a single vulnerability. For example, if an organization relies on employees teleworking because of an issue at its primary site, relocating to a site with resilient communications and backup power capabilities may be a good backup option.

Each continuity option has its strengths and weaknesses. Organizations must consider which option is most appropriate to reduce vulnerabilities and mitigate risk based on their own circumstances. Organizations are also encouraged to customize and supplement these options to achieve a robust and resilient capability that ensures essential function performance.

7.4.1. DISTRIBUTION

The *Federal Mission Resilience Strategy* (FMRS) acknowledges that although it is imperative to retain capabilities and sites to relocate personnel and functions, this is not adequate when no-notice threats or disruptions occur. Proactive distribution of the continuity planning factors can instead be employed.

Organizations achieve distribution by diversifying the Staff and Organization, Equipment and Systems, Information and Data, and Sites needed to perform an essential function. Diversifying means single points of failure in these planning factors are identified and multiplied to create redundancy. The redundant factors are then distributed in ways that make it unlikely that a single threat or hazard could disrupt more than a small portion of them. This can include proactive physical relocation outside of a threat area and/or diversifying resources such as critical infrastructure, vital supply chains, and secure and redundant equipment and systems at each site where essential functions are performed.

Federal Mission Resilience Strategy

Organizations are encouraged to read the FMRS to determine how the “Assess, Distribute, and Sustain” planning model can best be implemented within the organization and what role the organization may play in implementing Federal Mission Resilience across the Federal Executive Branch.

Existing alternate sites should not be eliminated based on the FMRS. Instead, they should be considered and, where possible, used to distribute the day-to-day performance of essential functions. This proactive distribution enables a rapid transfer of operations and command and control from one affected site across multiple unaffected sites with little disruption, without relocating personnel, and with downtime reduced to as near zero as possible.

This requires leadership to fully integrate their organization's continuity planning with preparedness, enterprise risk management programs, and personnel management processes. This integration optimizes the day-to-day use of mobile work, directed work, and telework (discussed below) and existing primary and alternate sites to achieve a natural distribution of Federal Executive Branch leadership and essential functions.

Distribution methodologies will—and should—differ across the Federal Executive Branch organizations based on the unique aspects of their missions, existing national footprint, resources (including budget), and the results of holistic organizational risk assessments, among many other factors. Accurate and appropriate orders of succession and delegations of authority must be in place to ensure this can happen.

Distributed personnel can also support continuity work through mobile work, directed work, and telework. Mobile work refers to tasks performed while employees travel from one work location to another. Directed work refers to work performed at a location at which an employee is directed to work, other than the official worksite. This can be the employee's residence or another approved alternate work location. Leadership often determines that a directed work location is necessary for performing essential functions based on novel or unanticipated circumstances. Telework is a flexible work arrangement in which an employee situationally or routinely performs duties and responsibilities from an approved worksite but still reports to their agency worksite on a regular and recurring basis. It can provide critical support to sustain essential functions. Employees who participate in an approved telework program may be incorporated into the organization's continuity plan and may be leveraged during catastrophic emergencies.

Mobile Work, Directed Work, and Telework Requirements

Refer to *FCD: Federal Executive Branch Continuity Program Management Requirements* for specific mobile work, directed work, and telework requirements.

Although telework may be used to enhance continuity, it is voluntary. This, and the potential for communications and power outages, means it should not be relied on as the organization's only continuity option for an essential function. Telework is also not appropriate for continuity team positions that are likely to send, receive, or require access to classified information while performing their duties.

7.4.2. DEVOLUTION

Devolution is the transfer of statutory authority and responsibility from the organization's primary operating staff to other staff to maintain organizational command and control and/or perform essential functions when necessary. Devolution is different from other continuity options in that staff and organization do not devolve—essential functions devolve.

When selecting devolution, organizations must ensure the staff and organization to whom a function devolves have the appropriate knowledge, permissions, clearances, and abilities. The organization must prepare devolution leadership and staff to conduct continuity operations through its training and essential function evaluation efforts (e.g., exercises). Ensuring that appropriate delegations of authority are in place is vital to the success of this continuity option. Organizations should also consider developing support documentation such as training and job aids, standard operating procedures, desk guides, and handbooks.

The site chosen for devolution should be sufficiently distant from the organization's primary and alternate sites that it is unlikely to be affected by the same catastrophic event or emergency that is disrupting normal or relocated operations. The equipment and systems, including communications systems, at a site where essential functions would devolve exist primarily to perform different functions. Organizations must ensure these alternate equipment and systems are appropriate for maintaining the performance of the essential function.

All continuity planning factors required for devolution and any additional resources that may be needed should be pre-positioned and available within a tolerable timeframe. The organization's devolution counterpart must be able to assume command and control or perform essential functions as soon as possible, but not later than 12 hours after devolution plan activation. It must be able to direct or sustain operations for a minimum of 30 days, or until normal operations are resumed.

Organizations may devolve in the short term while other continuity personnel relocate to an alternate site. Additionally, organizations may choose to partially devolve by transferring responsibilities for some essential functions but distributing, relocating, or retaining others. Or they may choose to transfer responsibilities for different essential functions to different sites. Devolution may be used as a stand-alone continuity option or in tandem with any other option.

Devolution Requirements

Refer to *FCD: Federal Executive Branch Continuity Program Management Requirements* for specific devolution requirements.

7.4.3. RELOCATION

Relocation is the movement of pre-identified members of an organization's primary operating staff from their primary site to an alternate site to continue performing essential functions when normal operations are disrupted. This includes essential function performance as well as command and control.

When selecting relocation, organizations should ensure the alternate site is sufficiently distant from the primary site that it is unlikely to be affected by the same catastrophic event or emergency that is driving operations from the primary location. Organizations should consider sites that are not uniquely susceptible to natural disasters. They should also select sites in areas that have access to power, telecommunication services, and the internet that are separate from the grids of the primary site, whenever possible. The offices responsible for these services in each organization can provide this information.

Organizations must provide the capability for continuity personnel to be fully operational at alternate locations as soon as possible, but not later than 12 hours after a continuity activation, and sustained for a minimum of 30 days following the occurrence of an emergency or until normal operations are resumed.

If feasible, organizations should consider maintaining multiple sites. Organizations may offset some of this cost and residual risk by using alternate sites on a daily basis and reducing their footprint at a primary site. Organizations are also encouraged to explore shared use possibilities with external organizations. Ultimately, the Organization Head is responsible for deciding which alternate sites will be used to ensure continued execution of the organization’s MEFs and PMEFs.

A benefit of relocation is that the organization’s primary operating staff can continue performing the essential functions they perform during normal operations. They are familiar with their roles and responsibilities and possess the appropriate knowledge, permissions, clearances, and abilities. They understand the processes of the essential function and what information and data they require. Ensuring that appropriate orders of succession and delegations of authority are in place is vital to the success of this continuity option.

Organizations should consider that the reactive nature of relocation is not well suited to no-notice events. Supplementing relocation with other continuity options like distribution and devolution may be required to achieve essential function resilience.

Relocation Requirements

Refer to *FCD: Federal Executive Branch Continuity Program Management Requirements* for specific relocation requirements.

7.4.4. HARDENING

Hardening is the systematic identification and reduction of vulnerabilities found in any of the continuity planning factors (Staff and Organization, Equipment and Systems, Information and Data, and Sites). Hardening may be used in conjunction with other continuity options or when other options are not feasible.

For example, to reduce staff and organizational vulnerabilities, organizations should ensure that appropriate orders of succession and delegations of authority are in place for leadership and key personnel. If continuity personnel rely on public transportation to reach an alternate site, organizations should develop alternate, contingency, and emergency transportation plans to reduce that vulnerability during an emergency that disrupts mass transit. Organizations should also maintain a comprehensive training program, along with realistic exercises to expose areas for improvement, and provide documentation such as training and job aids, standard operating procedures, desk guides, and handbooks.

As referenced in the BPA section of this FCD, CISA's *Resilient Power Best Practices for Critical Facilities and Sites* includes authoritative information on hardening sites. The ISC's *The Risk Management Process: An Interagency Security Committee Standard* establishes a single, formalized process when determining federal site security requirements.

As operations rely ever more heavily on ICT, hardening these and other vital equipment and systems becomes ever more important. Resources like CISA's Shields Up campaign and complementary Shields Ready campaign provide pertinent guidance. The Department of Commerce National Institute of Standards and Technology (NIST) offers a suite of mutually supporting publications focused on engineering cyber resilience.[14]

Information and data must also be hardened. Organizations should have multiple copies of their essential records in several locations stored on redundant media and in virtual storage environments. Organizations can consult resources provided by NARA for information about essential records and records recovery after a disaster or an emergency.

Hardening can be used across the continuity planning factors and to supplement other continuity options, but in some instances, it is the only option available to ensure the performance of the essential function. If a function requires a specific piece of equipment that cannot easily be reproduced at a different site, or if the function is geographically tied to the site where it is primarily performed, hardening may be the only continuity option available.

Hardening should be used as a stand-alone continuity option only when other options are not feasible, but it has some advantages. One is that the staff and organization charged with the day-to-day performance of an essential function continue to perform that function at a site and with equipment and systems optimized for that function. Another advantage is that hardening can delay the impacts of a threat or hazard long enough to endure short-term disruptions or find other, ad hoc mitigation solutions.

[14] NIST Computer Security Resource Center | CSRC

7.4.5. RISK MITIGATION BY CONTINUITY PLANNING FACTOR

Threat/hazard-specific mitigation is appropriate for well-understood and higher-probability threats and hazards, but emerging and future threats and hazards are best managed by adopting all-hazards vulnerability reduction approaches. Table 3 provides examples of threat-agnostic, impact-specific, all-hazards vulnerability reduction approaches.

Table 3: Risk Mitigation by Continuity Planning Factor

Staff and Organization	Equipment and Systems	Information and Data	Sites
Staff within an organizational structure who are required to individually and collectively support or perform the essential function	Physical resources or digital applications required to support the accomplishment of the essential function	The information and data required to complete or that result from the performance of the essential function	The facilities needed where the essential function is coordinated or accomplished
▪ Personnel rosters ▪ Orders of succession ▪ Delegations of authority ▪ Personnel preparedness ▪ Geographically distributed personnel	▪ Reserve supplies ▪ Supply chain resilience ▪ Resilient communications ▪ Hardened equipment and systems ▪ Infrastructure failure contingency planning ▪ Backup servers	▪ Hard copies/ external drives/ organization-approved USB flash drives ▪ Data management process/ procedures ▪ Redundant media and virtual storage environments ▪ Cybersecurity	▪ Facility security measures at alternate sites ▪ Alternate sites ▪ Distributed sites ▪ Telework or remote work capability

7.5. Documentation and Prioritization

After completing a BPA and BIA and selecting continuity options, organizations should document, prioritize, and submit updated MEFs for leadership approval using the steps provided below. Approved and prioritized MEFs enable organizations to perform effective continuity planning and effectively allocate the continuity planning factors and other resources required to perform MEFs.

Step 1: Complete MEF Data Sheets.

Organizations must finalize the documentation of each MEF.

Annex A Resources

Organizations may continue using the Mission Essential Function Data Sheet (Annex A, Form 2) to record information about their MEFs or develop data sheets of their own.

The MEF Data Sheets include the following information based on the BPA and BIA:

- **Organization:** The name of the organization responsible for the performance of the MEF.
- **Mission Owner:** The senior accountable government position with the original or delegated authority to lead the planning, programming, budgeting, execution, and associated risk management of the MEF.
- **MEF Statement:** A short statement that briefly describes the action to be conducted and why that function is mission essential. The MEF statement is generally one sentence.
- **MEF Narrative:** A comprehensive explanation of how the MEF facilitates the performance of the organization's mission and why that function is mission essential. The narrative may be multiple paragraphs, depending on the complexity level of the MEF, and must describe the function so that nonexperts may gain a reasonable understanding of what it does and does not include. The BPA will address the specific details of how the MEF is performed, so that information does not need to be included in the MEF narrative. The MEF narrative must include:
    - The statute, regulation, presidential directive, or other legal authority requiring the conduct of the MEF;
    - The products or services (outputs) provided because of performing the MEF; and
    - The actions the organization must perform to accomplish the MEF.
- **Impacts if Not Conducted:** A short explanation of the impact of not performing or delaying the performance of the MEF. This statement, which may be only a few sentences long, articulates why this function is mission essential.
- **Supported PMEF/MEF:** If the organization believes any of its MEFs support or implement a PMEF, it may identify these PMEFs on the MEF Data Sheet. If the organization believes any of its MEFs are PMEFs, it should instead submit those MEFs to the IAB as candidate PMEFs in a process described in the Candidate PMEF Submission section of this FCD. Although some MEFs could be associated with multiple NEFs, it is important to select the single NEF that it most directly supports. Most MEFs will not support a NEF and exist only to meet organizational mission requirements.
- **MTD and Degradation:** A statement that affirms whether the MEF must be performed continuously or how quickly it must be resumed if disrupted, as well as whether and how performance may be limited or otherwise degraded without compromising the organization's mission. The MTD and degradation will inform continuity planning and resource and budget considerations.

- **External Dependencies:** The external partners and stakeholders necessary to ensure successful MEF performance and the associated dependencies. Remember, external dependencies exist outside of the organization’s statutory or legal authority.
- **Point of Contact:** The individual within the organization who will provide follow-up information as needed. Organizations must include a name, title, email address, and phone number.

Step 2: Review and Submit Updated MEFs for Leadership Approval.

The process for submitting MEFs for final leadership review and approval and the composition of the MEF submission packages will vary based on individual organizational requirements. The package should include MEF Data Sheets and appropriate supporting material to enable leadership to make an informed decision on MEF approval.

Annex A. Forms

Form 1. Organizational Functions Worksheet

Government Function (Cite Source) and Mission Owner	Organizational-level Mission It Supports (Cite Source)	Outputs	Essential (X)	Non-essential (X)	MEF (X)
			□	□	□
			□	□	□
			□	□	□
			□	□	□
			□	□	□
			□	□	□
			□	□	□

Form 2. Mission Essential Function Data Sheet

MEF Data Sheet Date: _______________
Department/Agency:
Mission Owner:
MEF Statement:
MEF Narrative:
Impacts if Not Conducted:
Supported PMEF:
MTD/Degradation:
Dependencies and Interdependencies:
Point of Contact:

Form 3. Business Process Analysis Data Sheet – MEF

Business Process Analysis Data Sheet
Title/Statement:
Outputs (Step 1):
Leadership (Step 2):
Staff (Step 3):
Equipment and Systems (Step 4):
Information and Data (Step 5):
Site (Step 6):
ESAs (Step 7)
External Dependencies (Step 8):
Narrative (Step 9):
Budgeting (Step 10):
BPA Validated by (Step 11):

Form 4. Business Impact Analysis/Risk Assessment Worksheet

Title/Statement:								
Risk ID	Description	Likeli-hood #	Vulnerability Narrative	Vuln. #	Impacts Narrative	Imp. #	Risk #	Continuity Option(s)

Form 5: Candidate Primary Mission Essential Function Worksheet

Candidate Primary Mission Essential Function Worksheet

Date: MM/DD/YYYY

Department/Agency PMEF #

Candidate PMEF # and PMEF Short Title: Fewer than 68 characters, using complete words, including spaces and punctuation marks (the character total is limited to accommodate the NEF-PMEF Alignment Chart).

Candidate PMEF Statement: This is a complete one-sentence statement summarizing the unique function of the PMEF using common language.

Description of the Candidate PMEF's Alignment to a Specific NEF: Using complete paragraphs and sentence structure, provide the following:

1. Identification of the aligned NEF (a separate worksheet is required if the candidate PMEF contributes to more than one NEF; one worksheet is required for each NEF the PMEF supports).
2. Description of the candidate PMEF's specific output or outcomes (output/outcomes must be in plain language and describe how the candidate PMEF directly contributes to the NEF).
3. Summary of the candidate PMEF's process (using plain language, state how the PMEF achieves its output/outcomes).
4. Identification of candidate PMEF's interdependencies with external organizations (for example, other departments/agencies [D/As], foreign governments, the private sector, and nongovernmental agencies [NGOs]).
5. Description of how the candidate PMEF is unique to the D/A.
6. Description of the candidate PMEF's composition, addressing if the candidate PMEF is a "MEF bundle" or a "single-scope MEF" (we expect this to be D/A and functionally dependent).
7. Identification of significant changes to the candidate PMEF, if any, from previous cycle submission.
8. Identification of implications (functional and political) if the candidate PMEF is not conducted (using plain language, state a short and specific explanation of the impact if the PMEF fails).

Candidate Primary Mission Essential Function Worksheet

Date: MM/DD/YYYY

Department/Agency PMEF #

Summary of Candidate PMEF Assurance: Using complete paragraphs and sentence structure, provide the following:

1. Date of the last D/A continuity plan review/update.
2. Brief description of the sustainment of PMEF continuity methodologies and risk management. Depending on D/A and PMEF requirements, this may include the following: a description of the use of relocation and alternate facilities, a description of devolution implementation, remote work/telework implementation/applicability, information and communications technology (ICT) assurance measures such as testing programs and schedules of equipment refreshes, training and evaluation efforts, and external D/A dependencies necessary to PMEF performance and assurance.
3. Any identified links to D/A strategic plans and budget allocation.

Legislative or Directive Requirements for Candidate PMEF Narrative: Using complete paragraphs and sentence structure, provide the legislative or directive requirements for the PMEF, if applicable (noting that because PMEF constructs are based on MEFs, which have legislative or directive requirements, PMEFs based on MEF-level legislative or directive requirements may state this and list MEF requirements below).

Identification of Supporting Mission Essential Functions (PMEF inputs = the MEF[s] that constitute the PMEF):

1. Summary of supporting MEF(s), including the following:

   a. MEF name and D/A name designation;

   b. MEF statement;

   c. Legislative or directive requirements creating the MEF;

   d. Date of last supporting continuity plan(s) review, including identification of MEF risk management (such as a description of MEF assurance methodology and identification of maximum tolerable downtimes [MTDs] or measurements of acceptable tolerances for MEF degradation);

   e. Identification of MEF interdependencies with external organizations (other D/As, foreign governments, the private sector, and NGOs); and

   f. Responsible MEF component/office and contact information.

   (*Note:* This information is found in the recommendations for developing MEF Data Sheets in Section 7.5 of this FCD.)

2. MEF information will be added for each MEF as described in the previous list entry.

Candidate Primary Mission Essential Function Worksheet **Date: MM/DD/YYYY** **Department/Agency PMEF #**
D/A Candidate PMEF Package Point of Contact (staff-level point of contact/compiler for general questions regarding the worksheet): Name, Component/Office, Position, Contact Information
D/A Candidate PMEF Assurance/Continuity/Resilience Point of Contact (D/A Continuity Manager-level or Continuity Coordinator-level point of contact for general questions regarding continuity of the PMEF): Name, Component/Office, Position, Contact Information
D/A Candidate PMEF Mission Owner (Performance/Operations) Point of Contact (D/A Mission Owner-level point of contact for general questions regarding the PMEF performance/operations): Name, Component/Office, Position, Contact Information
D/A Candidate PMEF Package Approval (D/A Deputy-level or higher PMEF package approver): Name, Component/Office, Position, Contact Information

This page intentionally left blank

Annex B. Authorities and Resources

Authorities

Homeland Security Act of 2002, as amended (6 United States Code [U.S.C.] § 101 et seq.).

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

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

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

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

Executive Order 12977*, Interagency Security Committee,* Oct. 19, 1995.

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

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

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

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

National Security Presidential Memorandum 28, *National Operations Security Program*, Jan. 13, 2021.

Federal Mission Resilience Strategy, Dec. 7, 2020.

Resources

Cybersecurity and Infrastructure Security Agency, Binding Operational Directive (BOD) 18-02, *Securing High Value Assets*, May 7, 2018.

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

Cybersecurity and Infrastructure Security Agency, *Resilient Power Best Practices for Critical Facilities and Sites with Guidelines, Analysis, Background Material, and References*, November 2022.

Cybersecurity and Infrastructure Security Agency, *Vendor Supply Chain Risk Management (SCRM) Template*, April 2021.

Department of Homeland Security/Federal Emergency Management Agency, *Continuity Guidance Circular*, February 2018.

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

Department of Homeland Security/Federal Emergency Management Agency, FCD-1, *Federal Executive Branch National Continuity Program and Requirements*, June 2017.

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

Interagency Security Committee, *The Risk Management Process: An Interagency Security Committee Standard*, Dec. 1, 2021.

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

National Counterintelligence and Security Center, *Supply Chain Risk Management: Reducing Threats to Key U.S. Supply Chains*, October 2020.

National Institute of Standards and Technology, *Key Practices in Cyber Supply Chain Management: Observations from Industry*, February 2021.

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

Office of Management and Budget, Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 2016.

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

Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, Feb. 5, 2024.

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

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

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

Annex C. Definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Digital Application – 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 [NIST]).

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

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

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

Emergency Operating Records – Records an organization needs to continue functioning or to reconstitute after an emergency (Source: National Archives and Records Administration [NARA]).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

High Value Asset (HVA) – "Information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have a serious impact on the organization's ability to perform its mission or conduct business" (Source: Cybersecurity and Infrastructure Security Agency [CISA], *CISA Insights: Secure High Value Assets [HVAs]*).

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

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

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

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

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

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

Maximum Tolerable Downtime (MTD) – The longest amount of time an essential function may be disrupted before it results in unacceptable degradation of the mission it accomplishes (Source: FEMA).

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

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

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

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

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

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

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

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

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

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).

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

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

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

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

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

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

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

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).

Recovery Point Objective (RPO) – The point in time, prior to a disruption, at which data can be recovered. RPO informs backup frequency, and a higher RPO translates to a higher percentage of data retention/recoverability following a disruption (Source: FEMA).

Recovery Time Objective (RTO) – The maximum amount of time that information and data can be unavailable before it negatively impacts its function (Source: FEMA).

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

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

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

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

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

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

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

Risk Assessment – A product or process that collects information and assigns values to risks for the purpose of informing priorities, developing or comparing 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 [organizational] policy, order, or regulation if there is no applicable executive order, other presidential directive, or statute in the event of a vacancy in office or a position holder dies, resigns, or is otherwise unable to perform the functions and duties of that pertinent position” (Source: PPD-40, *National Continuity Policy*).

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

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

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

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

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

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

Annex D. Acronyms

APHS/CT	Assistant to the President for Homeland Security and Counterterrorism
BIA	Business Impact Analysis
BOD	Binding Operational Directive
BPA	Business Process Analysis
CAG	Continuity Advisory Group
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive
CFO	Chief Financial Officer
C.F.R.	Code of Federal Regulations
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
COG	Continuity of Government
D/A	Department and Agency
DHS	Department of Homeland Security
ECG	Enduring Constitutional Government
EOP	Executive Office of the President
ESA	Essential Supporting Activity
FCD	Federal Continuity Directive
FEMA	Federal Emergency Management Agency
FMRS	Federal Mission Resilience Strategy
FOUO	For Official Use Only
HQ	Headquarters
HVA	High Value Asset

IAB	Interagency Board
ICT	Information and Communications Technology
ICWG	Interagency Continuity Working Group
INFOSEC	Information Security
ISC	Interagency Security Committee
IT	Information Technology
MEF	Mission Essential Function
MTD	Maximum Tolerable Downtime
NARA	National Archives and Records Administration
NCC	National Continuity Coordinator
NEF	National Essential Function
NGO	Nongovernmental Organization
NIST	National Institute of Standards and Technology
NSPM	National Security Presidential Memorandum
NTER	National Threat Evaluation and Reporting
OMB	Office of Management and Budget
ONCP	Office of National Continuity Programs
OPM	Office of Personnel Management
OPSEC	Operations Security
OSTP	Office of Science and Technology Policy
PMEF	Primary Mission Essential Function
PPD	Presidential Policy Directive
RPO	Recovery Point Objective
RTO	Recovery Time Objective

S	Secret
SAOP	Senior Agency Official for Privacy
SCI	Sensitive Compartmentalized Information
SCRM	Supply Chain Risk Management
SLTT	State, Local, Tribal, and Territorial
TDY	Temporary Duty
THIRA	Threat and Hazard Identification and Risk Assessment
TS	Top Secret
U	Unclassified
U.S.C.	United States Code
USPS	United States Postal Service
WMD	Weapon of Mass Destruction