U.S. Department of Homeland Security
Federal Emergency Management Agency
Federal Continuity Directive 2
Issue Date: June 13, 2017

Federal Continuity Directive 2

Federal Executive Branch
Mission Essential Functions and
Candidate Primary Mission Essential Functions
Identification and Submission Process

Table of Contents

I. Purpose

Federal Continuity Directive-2 (FCD-2) implements the requirements of FCD-1, Annex B (*Essential Functions*), and provides direction and guidance to Federal Executive Branch Departments and Agencies (D/As) to assist in validation of Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs). The update and validation of essential functions includes conducting a comprehensive Business Process Analysis (BPA) to understand those processes necessary to the performance of organizational functions and requirements. It also includes conducting a Business Impact Analysis (BIA) to identify potential impacts on the performance of essential functions and the consequences of failure to sustain them. Further, it requires the application of organization-wide risk analysis to inform decision making and strengthen operations through effective risk management. FCD-2 outlines requirements and provides checklists and resources to assist D/As in identifying and assessing their essential functions through a risk-based process and in identifying candidate PMEFs that support the National Essential Functions (NEFs). This FCD provides guidance for conducting a BPA and BIA to identify essential function relationships, dependencies, time sensitivities, threats, vulnerabilities, consequences, and mitigation strategies related to the performance of the MEFs and PMEFs. This FCD also provides direction on the formalized process for submitting D/As' candidate PMEFs in support of the NEFs.

II. Applicability and Scope

The provisions of this FCD apply to the executive D/As enumerated in 5 United States Code (U.S.C.) § 101, including the U.S. Department of Homeland Security (DHS), independent establishments as defined by 5 U.S.C. § 104(1), government corporations as defined by 5 U.S.C. § 103(1), and the United States Postal Service. The D/As, commissions, bureaus, boards, and independent organizations are hereinafter referred to as "organizations" to better reflect the diverse organizational structures within the Federal Executive Branch. The provisions of this FCD are applicable at all levels of Federal Executive Branch organizations regardless of their location, including regional and field locations. Headquarters (HQ) elements are responsible for providing oversight and promulgating direction to their component, subcomponent, and field organizations. In this FCD, the term "headquarters" refers to the central, head offices of operations for organizations identified in Presidential Policy Directive (PPD)-40, Annex A, *Categories of Departments and Agencies*. The terms "component" or "subcomponent" refers to all organizational elements, whether at HQs or a regional, field, or satellite office.

Though not a requirement, state, local, tribal, and territorial governments, non-government organizations, and private sector critical infrastructure owners and operators are strongly encouraged to adopt this approach, as there are many dependencies and interdependencies among various levels of government critical to ensuring the continued functioning of governments and the continued performance of essential functions. Specific guidance for non-federal organizations is available in the Continuity Guidance Circular.

III. Supersession

This FCD rescinds and supersedes FCD-2, *Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process*, dated July 2013.

IV. Policy and Background

PPD-40, *National Continuity Policy*, sets forth the policy of the United States to maintain a comprehensive and effective continuity capability through Continuity of Operations (COOP), Continuity of Government (COG), and Enduring Constitutional Government (ECG) programs ensuring the preservation of government structure under the United States Constitution and continuing performance of NEFs under all conditions.[1]

As noted in FCD-1, national continuity programs are based on the continuous performance of NEFs through the sustainment of essential functions performed by D/As. NEFs are the foundation of all continuity programs and capabilities and represent the overarching responsibilities of the Federal Government to lead and sustain the Nation before, during, and in the aftermath of a catastrophic emergency. All D/As, regardless of size or location, are required to have a viable continuity capability to ensure organizational resilience and continued performance of essential functions under all conditions. The foundation of robust and viable continuity programs and capabilities is the understanding and commitment to the continued performance of the organization's essential functions. Organizations must consider and fully integrate continuity planning and procedures into all aspects of daily operations to create a culture of continuity that will ensure seamless continuation of essential functions under all conditions.

To preserve the government and sustain the NEFs, D/As must identify their MEFs and PMEFs and ensure that those functions can be continued during, or resumed rapidly after, a disruption to normal operations. While the Federal Government provides many services to the American people, Federal Executive Branch D/As must identify and prioritize those critical services that must continue during an emergency. D/As must set those priorities as part of their preparedness posture and not wait for a crisis or a continuity event to determine which activities must be sustained throughout the event. Only with a coordinated, organization-wide approach can D/As ensure resilience and the ability to continue to perform essential functions during both catastrophic emergencies and more routine disruptions to operations both planned and unplanned.

FCD-2 directs updates to and validation of essential functions, requiring the conduct of a comprehensive BPA, conduct of a BIA, and the application of agency-wide risk analysis in support of organizational resilience and continuity programs. This analytic approach defines how robust an organization's continuity program shall be and underscores that strengthening the continuity program will strengthen the enterprise, making the organization more resilient regardless of the challenges it may face. Risk analysis of a BPA, supported by a BIA, aids in the identification on non-obvious, emerging, and future risks or threats to an organization's operations. Structured and in-depth analysis enables organizations to consider and allocate

[1] Presidential Policy Directive-40, *National Continuity Policy*, July 15, 2016, p. 4.

resources to those areas of greatest risk and where the most benefit from investment may be achieved. Analytic findings and supporting documentation further enable justification of needed resources, as well as determinations on resource allocation throughout the organization. Investing in those areas critical to the performance of an organization's essential functions will further allow agencies to build resilience and more readily adapt to evolving threats. The use of analysis and related tools will maximize the organization's use of resources given dependency considerations for performance of both steady-state functions and essential functions during a catastrophic emergency.

V. MEF and Candidate PMEF Identification

Identification and prioritization of essential functions enable effective continuity planning. Essential functions are critical activities used to identify key assets, supporting tasks, and resources that an organization must include in its continuity planning process. Essential functions are those functions an organization must continue in a continuity situation, whether the functions are PMEFs, MEFs, or Essential Supporting Activities (ESAs). Annex A describes the types of essential functions and Annexes B through E provide direction and guidance on the processes for identifying, reviewing, validating, and updating MEFs and PMEFs and conducting a BPA and BIA.

Many D/As have MEFs and a smaller number of D/As have PMEFs. This narrowing and prioritizing is both appropriate and consistent with the concepts that underpin a comprehensive continuity policy. The fact that some D/As may not have a PMEF is not a reflection of the importance of their responsibilities, but rather a reflection of the urgency of the functions that D/As may need to perform during a catastrophic emergency. D/As' analysis should include consideration of functions performed at all of the organization's locations and not be limited to HQ activities.

VI. Risk Management and Analysis

Risk is the "potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences."[2] An agency-wide continuity risk management program will inform agency planning and resource allocation decisions to sustain essential functions, build on the organization's existing risk management activities, and encompass all of the organization's operations. Countless risks may cause degradation or hindrance in the performance of essential functions, supporting activities, and normal operations. Performing analysis to better understand these risks and then managing risks to minimize their effects is critical. Examining factors within an organization's operating environment that exhibit the potential to disrupt business processes through the exploitation of vulnerabilities will aid in the prioritization of risks and associated risk management.

Analyzing risk to the organization – the *enterprise* – requires detailed knowledge of the organization's operations, information on what may cause harm and the results of such harm, and information on how to contend with identified risks. Risk management and analysis requires a

[2] U.S. Department of Homeland Security, *DHS Risk Lexicon*, 2010 Edition, September 2010, p. 27.

team approach, leveraging subject-matter experts on an organization's operations, programs, and functions to develop a holistic picture of enterprise risk and an understanding of dependencies, interdependencies, and interfaces.

A. Risk Analysis

Various types of analysis will contribute to the overall understanding of the risks faced by an organization and how to best manage those risks. Enterprise risk management may inform decision making involving organizational strategic and operational planning, human capital planning, capital investment planning, program management, and budget formulation. Programmatic risk analysis considers the technological or quality, cost, and schedule risks within a program. All-hazards risk analysis considers risks posed by all conditions, environmental or manmade, that have the potential to cause injury, illness, or death; damage to or loss of equipment, infrastructure services, or property; or causing functional degradation. Although there are many ways to perform analysis, the following general steps apply:

- **Define** the context and develop the analysis by setting requirements and parameters, to include defining the scope of the analysis and building the analysis team.
- **Identify** the organization's essential functions, considering how the "system" works. Identify potential risks based on those functions.
- **Assess** the potential risks to the organization, looking at threats, vulnerabilities, and consequences.
- **Develop alternatives** to manage risks to an acceptable level, which may include accepting, avoiding, transferring, or controlling risk.
- **Prioritize (or rank and order)** the identified risks and risk management strategies, considering associated costs and benefits. Decide upon and implement appropriate strategies.
- **Evaluate and monitor** risk management strategies to determine and continuously improve upon risk mitigation.
- **Defend** prioritizations and resource allocations, based on the results of risk analysis, to enhance the readiness, preparedness, and resilience of the organization.

Risks must be communicated to improve understanding among an organization's leadership, staff, and key stakeholders, enhance risk perception, and support risk management decisions and resource allocation. Risk analysis will inform continuity planning efforts and enable organizations to allocate resources to derive the most benefit from their investment.

B. Critical Infrastructure and Interdependency Analysis

The Nation's critical infrastructure provides services that underpin the performance of essential functions. This supporting infrastructure is both diverse and complex, and each of the 16 critical infrastructure sectors has unique characteristics, operating models, and risk profiles.[3] The term critical infrastructure is used to describe "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a

[3] For additional information on critical infrastructure sectors, see "Critical Infrastructure Sectors," U.S. Department of Homeland Security. https://www.dhs.gov/critical-intrastructure-sectors.

debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[4] Together, PPD-40 and PPD-21, *Critical Infrastructure Security and Resilience*, require the Federal Government to coordinate with state, local, territorial, and tribal governments and private sector owners and operators of critical infrastructure, as appropriate, to strengthen the Nation's resilience and sustain essential services during a catastrophic emergency.

As part of risk analysis, the analysis team must identify internal critical assets and systems supporting essential functions and external infrastructure upon which operations are dependent, including but not limited to "lifeline" infrastructure such as energy or power, water, communications, and transportation systems. Analyzing dependencies and interdependencies on critical infrastructure that support the performance of essential functions contributes to the organization's BIA and analysis of resilience. This information contributes to effective risk management to ensure the protection of critical assets, networks, systems, and information necessary to the performance of essential functions.

C. Analysis Outcomes

Analyzing risk and related dependencies on critical infrastructure through a BPA and BIA aids in the identification of non-obvious risks, gaps in an organization's operational processes and procedures, and essential function resource requirements. The BIA must take a risk-based approach to ensure all potential threats and hazards, vulnerabilities, and consequences are considered.

Through conduct of BPAs and BIAs, D/As must:

- Identify and prioritize essential functions and resource requirements.
- Determine dependencies and interdependencies related to the performance of essential functions.
- Identify and assess factors which may impact the performance of essential functions and the potential for cascading effects. D/As should consider existing threat assessments, vulnerability assessments, and consequence analysis, where available.

While organizations can neither respond to, nor eliminate, all risk, they must work to assess and manage challenges to perform essential functions based on structured and documented analysis. The determination and socialization of maximum tolerable downtimes, external dependencies upon critical infrastructure sectors or other organizations, and internal dependencies or interfaces will inform decisions on resource allocations and activities to sustain essential functions. Risk and dependency analysis inform mitigation actions needed to sustain essential functions and the development of the organization's continuity program. Collectively, the continuity community will gain an understanding of how essential functions are interrelated, how MEFs support PMEFs, and how PMEFs support NEFs to ensure the Nation can continue to function before, during, and after a catastrophic emergency. Effective risk management will strengthen organizational resilience, improve readiness, and enhance the Nation's resilience.

[4] Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience*, February 12, 2013, p. 12; USA Patriot Act of 2001, Section 1016(e), (42 U.S.C) 5195c(e)).

Annexes C and D outline the requirements, key considerations, and basic processes for conducting a BPA and BIA. However, given the wide range of structured analytic techniques and methodologies available, the specific methods used by D/As to conduct their BPAs and BIAs is ultimately up to individual organizations provided that the factors considered and documentation meet FCD-2 requirements.

VII. Submission Process Requirements

D/As must review biennially MEFs and supporting BPAs and document the dates of review and names of personnel conducting the review in accordance with FCD-1. D/As will follow the processes outlined in the annexes of this FCD to identify, review, and validate their MEFs, existing PMEFs, and candidate PMEFs. D/As must incorporate any identified changes generated by new programs, priorities, or functions within the organization and any organizational changes to existing programs or functions. D/As' analysis should include consideration of functions performed at all of the organizations' locations and not be limited to HQ activities. After the review and validation process, D/As will determine whether they need to revise an existing PMEF or propose a new candidate PMEF for consideration by the Interagency Board (IAB), established by the National Continuity Coordinator, following the submission guidance in Annex F.

VIII. Additional Guidance

FEMA National Continuity Programs will provide familiarization briefings and training on the MEF and candidate PMEF identification and validation process.

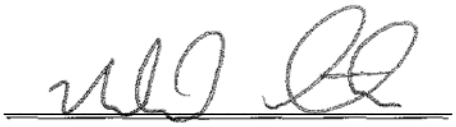
Annex J provides a list of references that may aid in the identification and validation of MEFs and PMEFs and performance of risk analysis.

IX. Point of Contact

Questions regarding this FCD can be submitted to FEMA National Continuity Programs at (202) 646-4145 or via email at FEMA-nationalcontinuity@fema.dhs.gov.

X. Distribution

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



6-13-17

Robert J. Fenton
Administrator (Acting), FEMA

Date

ANNEX A: DESCRIPTION OF FUNCTIONS

Federal Executive Branch continuity programs must support and provide for the continued performance of NEFs during a catastrophic emergency. D/As must validate and identify changes to PMEFs and MEFs to ensure that they appropriately support NEFs and that the D/A can perform or rapidly resume essential functions after a disruption to normal operations. While the Federal Government provides many services to the American people, it is important to establish priorities and allocate resources based on sound planning and risk-based analysis. The following list of functions better defines those services.

Government Functions: The collective functions of the Executive Office of the President and the executive D/As, as defined by statute, regulation, presidential directive, or other legal authority, and the functions of the legislative branch and judicial branch.[5]

Essential Functions: Subsets of Government Functions that are categorized as MEFs, PMEFs, and NEFs.[6]

NEFs: Select functions that are necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through COOP, COG, and ECG capabilities.[7]

Table A-1 lists the NEFs, which represent the overarching responsibilities of the Federal Government and are the primary focus of Federal Government leadership before, during, and in the aftermath of a catastrophic emergency.

PMEFs: Those MEFs that must be continuously performed to support or implement the uninterrupted performance of NEFs.[7]

MEFs: The essential functions directly related to accomplishing the organization's mission as set forth in its statutory or executive charter. Generally, MEFs are unique to each organization.[7]

ESAs: Functions that support performance of MEFs but do not reach the threshold of MEFs or PMEFs. ESAs are important facilitating activities performed by most organizations (e.g., providing a secure workplace, ensuring computer systems are operating); however, the sole performance of ESAs does not directly accomplish an organization's mission.[8]

[5] PPD-40, *National Continuity Policy*, July 15, 2016, p. 3.
[6] PPD-40, p. 2(h).
[7] PPD-40, p. 3.
[8] Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements*, January 17, 2017, p. B-1.

Table A-1. National Essential Functions[9]

National Essential Functions
NEF 1: Ensuring the continued functioning of our form of government under the United States Constitution, including the functioning of the three separate branches of government.
NEF 2: Providing leadership visible to the Nation and the world and maintaining the trust and confidence of the American people.
NEF 3: Defending the United States against all enemies, foreign and domestic, and preventing or interdicting attacks against the United States or its people, property, or interest.
NEF 4: Maintaining and fostering effective relationships with foreign nations.
NEF 5: Protecting against threats to the homeland and bringing to justice perpetrators of crimes or attacks against the United States or its people, property, or interests.
NEF 6: Providing rapid and effective response to and recovery from the domestic consequences of an attack or other incident.
NEF 7: Protecting and stabilizing the Nation's economy and ensuring public confidence in its financial systems.
NEF 8: Providing for Federal Government services that address the national health, safety, and welfare needs of the United States.

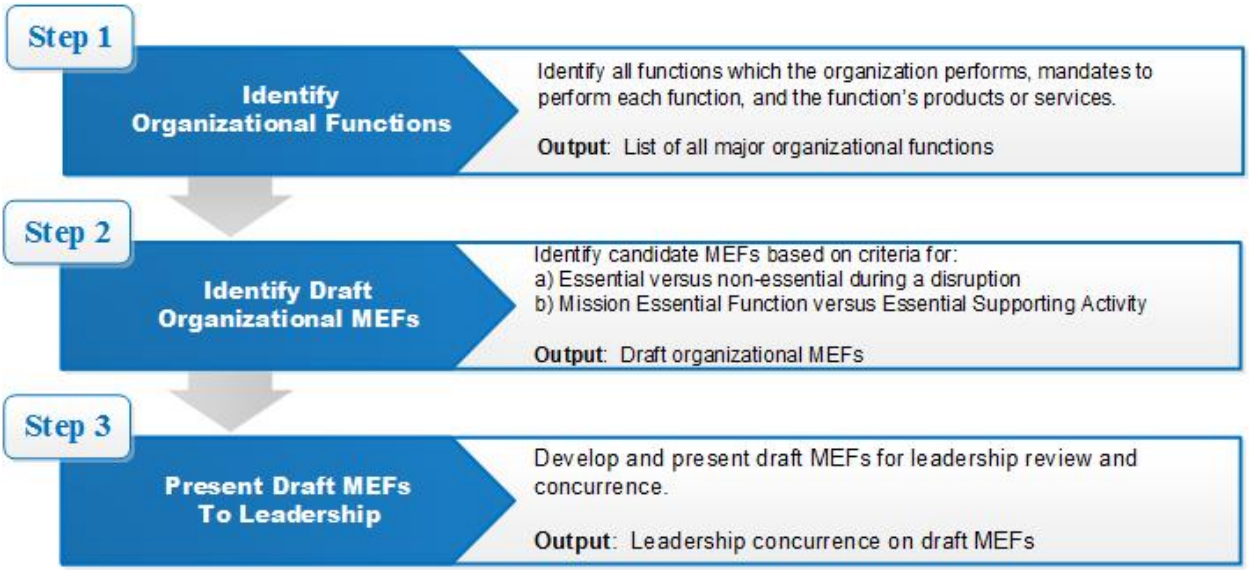
[9] PPD-40, pp. 4-5.

ANNEX B: MISSION ESSENTIAL FUNCTION IDENTIFICATION PROCESS

The proper identification of MEFs is critical to effective continuity planning. During a continuity event, key resources may be limited and personnel may be unavailable. D/As must consider these factors and validate assumptions when identifying, validating, and prioritizing MEFs.

The process described in Figure B-1 outlines a three-step process to support the identification, review, and initial validation of MEFs. The outcome of this process supports leadership concurrence of draft MEFs, enabling the development, review, and validation of essential functions through conduct of a BPA and BIA.

Figure B-1. Mission Essential Function Identification Process



Step 1: Identify Organizational Functions: In this step, an organization identifies and lists all major organizational functions that support performance of the D/A's mission. As part of this step, an organization may review and validate existing lists of organizational functions, as appropriate.

The list of organizational functions must include:

1. A description of each function in basic terms.
2. The requirement to perform each function, listing the applicable statute, regulation, presidential directive, or other legal authority.
3. The products or services delivered or actions each function accomplishes.

Examples of organizational function descriptions are listed below:

1. Protect critical infrastructure.
2. Maintain and ensure operational capability of D/As computer systems.
3. Provide medical services to veterans.

4. Manage facilities.
5. Lead national emergency response efforts during major disasters and emergencies.

D/As may use Annex G – Form 1, *Organizational Functions Worksheet*, for documenting the information collected during Step 1.

Step 2: Review or Identify Agency MEFs: After identifying and listing all major organizational functions that support the performance of its mission, organizations must review each identified function and determine which functions are potential new MEFs or updates to existing MEFs. Organizations should consider several factors when identifying MEFs.

1. Concurrently review existing MEFs and make necessary updates or validate information, as appropriate.
2. Review functions performed both at HQ and other locations where the organization's mission is executed.

D/As should assess MEF priorities to more effectively plan for the required resources and capabilities to perform the MEF(s) under all conditions (See Annex E *Documentation and Prioritization*). An understanding of essential and non-essential functions and of ESAs will aid in identifying priority functions.

MEFs versus Non-Essential Functions: When reviewing the list of organizational functions, a D/A must first identify whether a function is essential or non-essential. The distinction between these two categories is whether or not a D/A must perform a function during a disruption to normal operations and must continue performance during emergencies. Essential functions are both important and urgent. Functions that can be deferred until after an emergency are identified as non-essential.

MEFs versus ESAs: After determining whether the organizational functions are essential or non-essential, a D/A must determine if the essential functions are MEFs or ESAs. MEFs are the essential functions directly related to accomplishing the organization's mission as set forth in statutory or executive charter. Generally, MEFs are unique to each organization. ESAs are functions that support the performance of MEFs. ESAs are important activities performed by most organizations; however, the performance of ESAs alone does not accomplish an organization's mission. MEF's may be supported by multiple ESAs. Examples of MEFs and ESAs are provided in Table B-1.

Table B-1. Mission Essential Functions versus Essential Supporting Activities

Mission Essential Function	Essential Supporting Activity
Protect critical infrastructure	Maintain and ensure operational capability of the organization's computer systems.
Provide medical services to veterans	Manage facilities, including providing security.
Lead national emergency response efforts during major disasters and emergencies	Account for employees.
Collect intelligence	Manage the personnel payroll system to ensure all employees receive salary payments and employees receive appropriate pay and benefits.
Perform health inspections	Provide legal counsel to leadership and components on policy matters.
Operate satellites	Gather, coordinate, and disseminate information about programs, essential functions, and activities to the public.
Ensure food safety	Administer and provide guidance and counseling to employees for Title VII, Equal Employment Opportunity Program.
Regulate banking	Represent the agency on urgent department-level policy matters.

Organizations may use Annex G – Form 1, *Organizational Functions Worksheet*, to assist with identifying essential and non-essential functions and MEFs and ESAs.

Step 3: Initial Leadership Validation of MEFs: After completing Steps 1 and 2, an organization will have a list of its MEFs and ESAs. The organization should then present the list of updated, validated, or new MEFs and ESAs to leadership for initial review and concurrence. Obtaining concurrence or approval of MEFs and ESAs at this point allows an organization to proceed and conduct an efficient, effective, and targeted BPA and BIA of the identified essential functions.

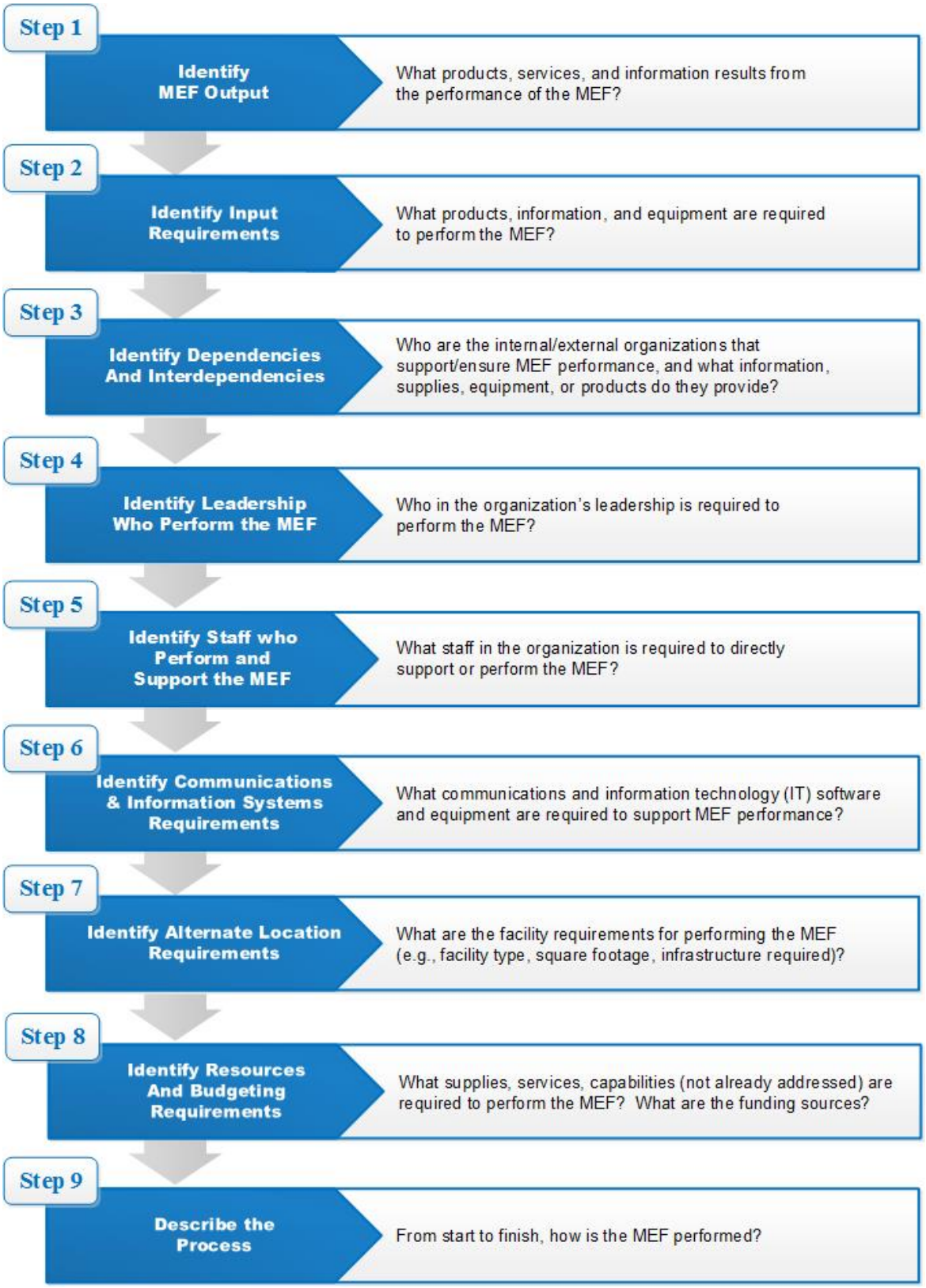
ANNEX C: BUSINESS PROCESS ANALYSIS

The BPA is a systematic method of examining, identifying, and mapping the functional processes, workflows, activities, personnel expertise, systems, data, interdependencies, alternate locations, and other resources needed to perform a MEF. The MEF identification process in Annex B identifies what essential functions an organization must continue, and the BPA process identifies how these essential functions are performed. Through BPAs, D/As must clearly describe how each MEF is performed, to include process flows and operational details, and identify appropriate resources that must be available during or immediately following a disruption to normal operations to enable the rapid resumption of MEF performance.

Conducting the BPA: The basic elements of a BPA are shown in Figure C-1. The BPA process is presented as steps, but this nine-step process is not prescriptive provided that all necessary elements are analyzed and documented as part of a BPA. The BPA requires an in-depth understanding of each identified MEF and the ability to describe and document each process element and required resources. The BPA also must include the identification of ESAs necessary to perform each MEF. D/As may consider additional steps or elements to ensure a comprehensive analysis and documentation of their organizations' MEFs, as appropriate.

D/As may use Annex G - Form 2, *Business Process Analysis Data Sheet*, to aid in documenting the BPA.

Figure C-1. Business Process Analysis Steps



Step 1: Identify MEF Outputs: This first step of the BPA is intended to identify products, services, and information (i.e., deliverables or outputs) that result from performance of the MEF. An organization also identifies the partners and stakeholders that receive the outputs. The description must include appropriate metrics that identify specific performance measures and standards, as the MEF output timeframes will inform the BIA.

Listed below are examples of MEF outputs:

1. Provide the public with emergency warnings of severe weather (U.S. Department of Commerce/National Oceanic Atmospheric Administration/National Weather Service).
2. Provide the President with information to support major disaster declaration decisions (DHS/FEMA).
3. Screen passengers arriving on international flights or ships prior to entry into the United States (DHS/Customs and Border Patrol).
4. Provide critical medical care to veterans and retired military personnel (U.S. Department of Veterans Affairs).
5. Inspect livestock to ensure the safety of the Nation's food supply (U.S. Department of Agriculture/Food Safety and Inspection Service).

Step 2: Identify Input Requirements: In this step, an organization identifies products, services, information, supplies, equipment, and other resources (i.e., inputs) required to perform the MEF and deliver the MEF outputs, which may be internal to the organization or depend on external partners. Organizations must identify what input is required, from whom, and when, as the input may be required at the beginning of MEF performance or as the functional process proceeds. The inputs description must include delivery time requirements, which will inform the BIA.

Listed below are examples of MEF inputs:

1. Situational awareness reports.
2. Damage assessments.
3. Requests for government assistance.
4. Direction from higher authority to perform a function.
5. Law enforcement support request.
6. Requests to inspect or repair infrastructure.

Step 3: Identify Dependencies and Interdependencies: This step focuses on identifying dependencies and interdependencies with partners and stakeholders required to perform the MEF, to include other government organizations, critical infrastructure owners and operators, non-governmental organizations, private sector organizations, and others as appropriate. The description must include information on the ability and expectations of dependent organizations to provide required inputs during a disruption to normal operations.

Below is an example of information to include for each interdependent relationship:

1. Organization name.
2. Description of organization.
3. Point of contact and contact information.
4. Type of information, data, services, and support provided.

5. Coordination requirements.
6. Timelines for providing information, data, services, and support, as appropriate.
7. Information on the provision of inputs during a disruption to normal operations and activation of the organization's continuity plan. Outline relevant plans and any memoranda of agreement in place for support during a disruption.

Note: An important element to consider is whether organizations understand their input is necessary for another organization's performance of an essential function.

Step 4: Identify Leadership Who Perform the MEF: This step identifies organizational leadership required to make decisions and perform other key actions necessary to perform the MEF. The description must include the location of appropriate senior leadership, specifically if their action can be performed remotely or they are needed at a certain facility, as well as communication requirements to support MEF performance.

Listed below are examples of leadership requirements.

1. Decision to activate programs or reallocate resources for disaster response.
2. Decision to divert a satellite from its existing trajectory.
3. Decision to approve a new drug for general use.
4. Decision to draw down the Strategic Petroleum Reserve.
5. Decision to close federal facilities to the public.
6. Recommend a foreign policy change to the President.

Step 5: Identify Staff Who Perform and Support the MEF: In this step, an organization identifies staff required to perform the MEF. The description must include appropriate knowledge, skills, abilities, expertise, experience, certifications, licenses, and clearances or permissions needed and the number of staff required to perform the MEF.

Listed below are examples of staffing requirements:

1. Twelve (12) staff with Top Secret security clearances and situational awareness training to provide 24/7 operations center staffing.
2. Two (2) IT specialists experienced in the operations and maintenance of identified mission critical systems.
3. Four (4) licensed civil engineers experienced in road and bridge safety and inspection requirements.
4. Three (3) budget analysts capable of accounting for and processing emergency expenditures.

For agencies with multiple MEFs, annotate staff who may support more than one MEF to help avoid unnecessary duplication of resources.

Step 6: Identify Communications and Information Systems Requirements: In this step, an organization identifies communications and information systems required to perform its MEFs. The description must include specific capabilities or data needed, classification requirements, and any other unique requirements. The description must also include information on system dependencies and interfaces with other systems or data sources. For more information on D/A

continuity communications requirements, see Office of Science and Technology Policy/Office of Management and Budget Directive D-16-1, *Minimum Requirements for Federal Executive Branch Continuity Communications Capabilities.*

Listed below are examples of communications and information systems requirements:

1. Standard office equipment (e.g., unclassified telephones, facsimile machines, desktop/laptop computers).
2. Graphic printing and display equipment.
3. Secure phone with conference capability.
4. Land-mobile radio.
5. Unique software applications necessary to access critical records and databases and to process incoming data.

Step 7: Identify Alternate Location Requirements: This step identifies facility requirements needed to perform the organization's MEFs. The description must include space, configuration, security, safety, support services (e.g., lodging, food services, medical support), and storage requirements appropriate for the organization's operations.

Listed below are examples of alternate location requirements:

1. Operations center of 1,000 square feet of open space with 24/7 secure access.
2. Sensitive Compartmented Information Facility of 800 square feet with four workstations and meeting space.
3. General office space of 40,000 square feet.
4. Climate-controlled storage space of 4,000 square feet to accommodate files or supplies.

Refer to FCD 1, Annex G, *Alternate Locations*, for more information on this topic.

Step 8: Identify Resource and Budget Requirements: This step includes identifying resource and budget requirements to perform the MEF for up to 30 days following a continuity activation or until normal operations are resumed. Resources not yet captured in the BPA process may include standard operating procedures, essential records, and reference materials required for MEF performance. The description must include and account for funding requirements for all identified resources needed to perform the MEF and ESAs.

Step 9: Describe the Process: In this step, an organization develops a narrative description that captures all information gathered during Steps 1 – 8 and describes the process of performing the MEF. The organization will develop appropriate diagrams or other informational aids to support the narrative description. Documenting the process will not only describe how the MEF is accomplished but also will aid in validating the information compiled and limit omission of any details.

The BPA description of the process required for MEF performance will:

1. Inform the BIA.
2. Inform ongoing risk analysis and risk management.
3. Support the development, update, and validation of continuity plans and procedures.

4. Support the development, update, and validation of checklists for continuity of operations.
5. Support orientation and training of continuity team personnel and those responsible for devolution.

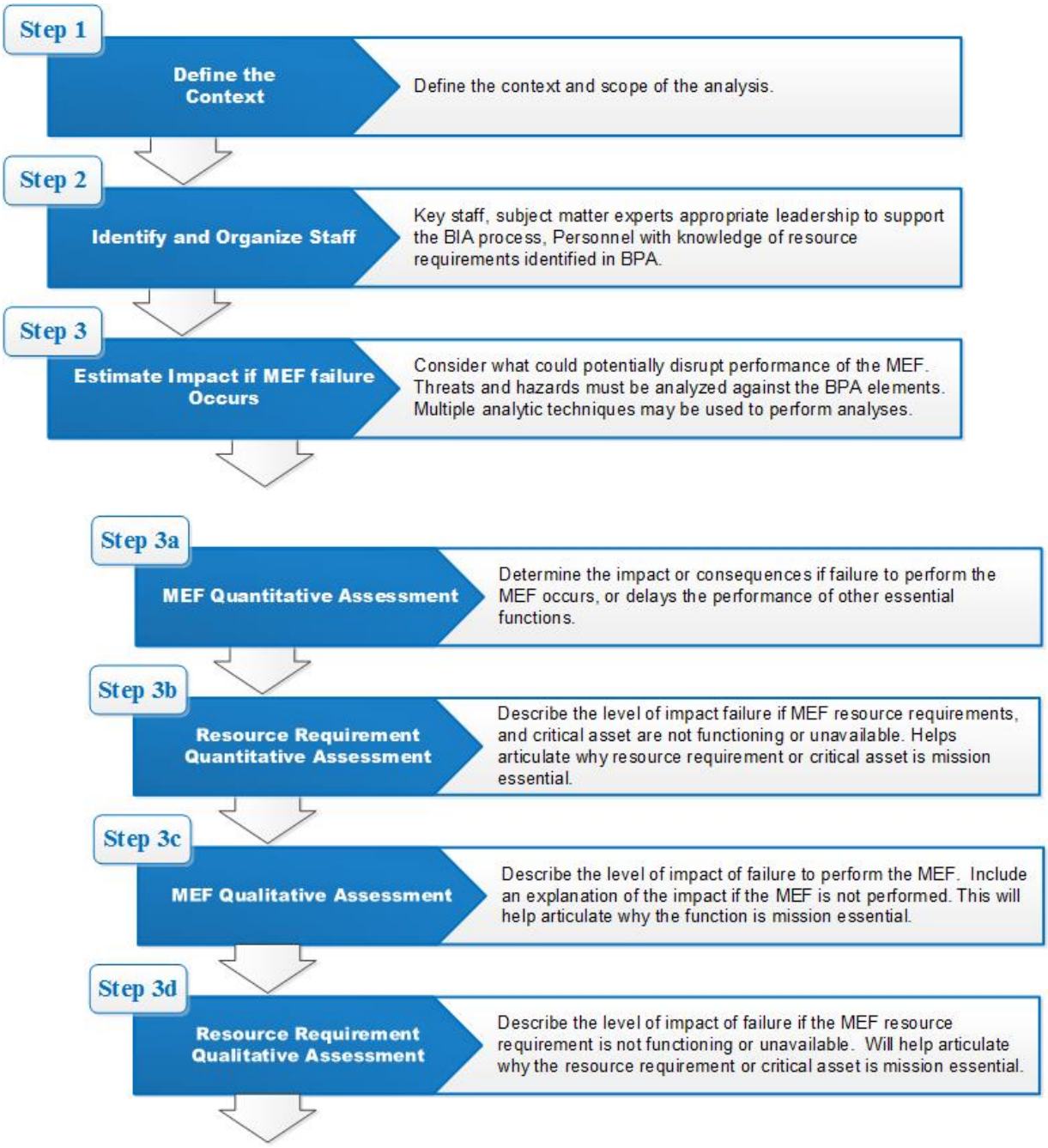
ANNEX D: BUSINESS IMPACT ANALYSIS

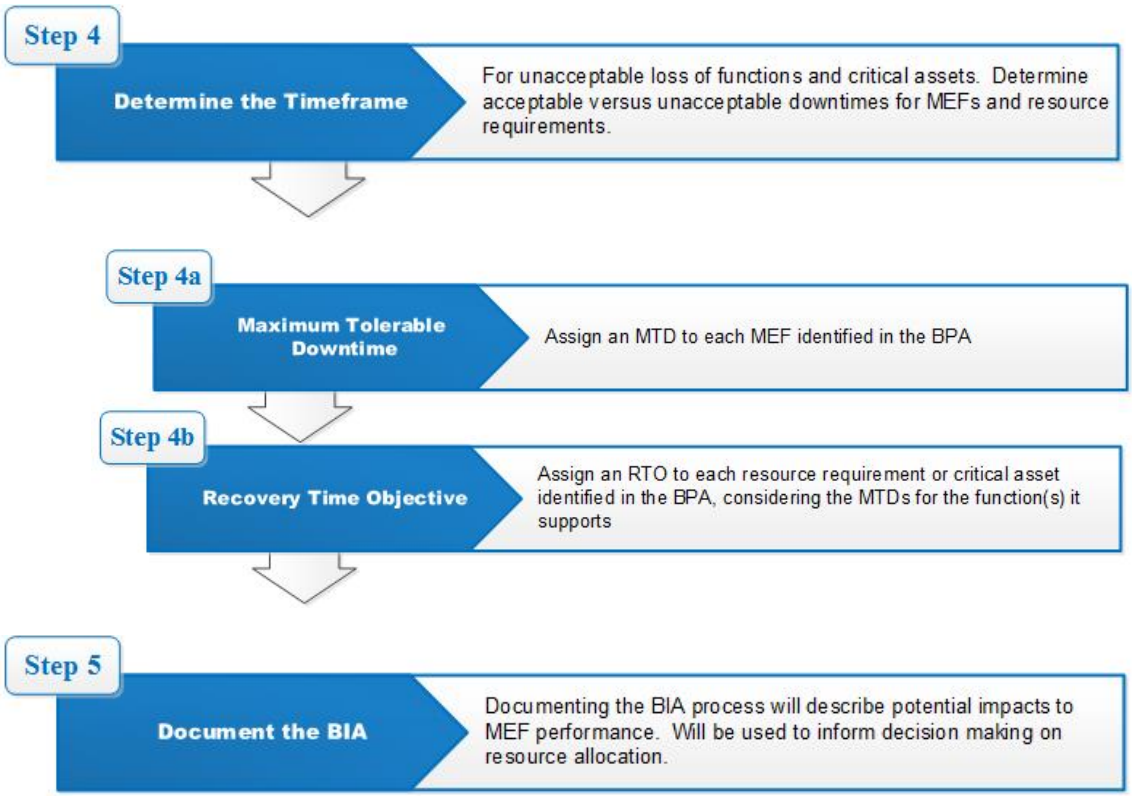
The BIA provides a method of identifying the potential negative impacts of failing to perform an essential function. D/As may leverage existing processes and internal analyses to support the BIA, provided the requirements outlined in FCD-1 and FCD-2 are met. D/As should also use the information derived during the BPA process to inform the BIA. It is used to assess comparative risk for MEFs and PMEFs, to include the processes and critical assets that support their performance, and informs broader risk analysis and risk management efforts. The BIA assists in the prioritization of essential functions and supporting resources, considering the consequences of their loss or degradation and their criticality to the organization's mission.

A formal review, update, and validation of the organization's essential functions through a BIA must be conducted at least every two years. As part of biennial continuity assessments conducted by FEMA, D/As must affirm that risks to the performance of its MEFs and PMEFs have been evaluated, and documented as part of its BIA.

BIA Process: The BIA process can generally be conducted in the steps presented in figure D-1, and may be tailored by D/As to ensure a comprehensive analysis of the consequences of failing to sustain essential functions. A separate analysis should be conducted for each MEF and the respective threats or hazards that may disrupt the performance of the MEF.

Figure: D-1. Business Impact Analysis





Step 1: Define the Context: The first step in the BIA process is to define the scope of the analysis. When scoping the requirements and constraints of this impact analysis, the organization must analyze the following variables:

1. The organization's essential functions.
2. The criticality of essential functions and supporting infrastructure and other resources.
3. Consequences and cascading effects of a degradation, disruption, or failure to perform essential functions and timeframes associated with those consequences.

D/As should determine other variables relevant to their organization in conducting risk analysis, to include:

1. Organizational risk management capabilities and resources.
2. The various partners and stakeholders involved in risk management.
3. The availability and quality of information on risks.
4. Constraining factors.

Step 2: Identify and Organize Staff: In this step, an organization identifies key staff, subject-matter experts, and appropriate leadership to support the BIA process. D/As must identify personnel with knowledge of each resource requirement identified in the BPA process and who are knowledgeable on all aspects of performing the MEF and ESAs. They must understand the criticality of the function, risks of its failure, and dependencies for MEF performance. Key personnel include, but are not limited to, those with expertise in program management, finance, communications and IT, facilities, emergency management, security, business operations, essential records, and risk analysis (various types).

Step 3: Estimate Impact if MEF Failure Occurs: D/As must consider what could potentially disrupt the performance of the MEF, to include terrorist and criminal threats, natural hazards, technological hazards, service disruptions, and various non-obvious risks. Table D-1 provides examples of threats and hazards. Applicable threats and hazards must be analyzed against the BPA elements, including interdependencies, to determine the extent of impacts of MEF failure.

Table D-1. Potential Threats and Hazards

Potential Threats and Hazards	
External Threats and Hazards	
• Explosions: - Nuclear Attack: Global War, Improvised Nuclear Device - Radiological Attack: Radiological Dispersal Device - Explosives Attack: Improvised Explosive Device - Incendiary Device	
• Active Shooter, Armed Assault	
• Chemical/Biological Events: - Biological Attack/Outbreak - Aerosol Anthrax; Plague; Ricin - Food Contamination - Animal Disease - Pandemic Influenza	 - Chemical Attack/Accident - Blister Agent - Nerve Agent - Toxic Industrial Chemicals - Chlorine Tank Explosion
• Infrastructure Attack/Failure/Damage: - Power Outage (Blackout) - Communications System Disruption - Transportation System Disruption - Water Supply Contamination, Sewage System Failure	 - Major Fire - Heating/Air Conditioning Failure - Ventilation System Failure
• Cyber Attack: - Loss of Data or Network Service Disruption	 - Control Systems Failure
• Economic/Labor/Insurrection: - Civil Unrest - Labor Dispute - Workforce Strike	 - Demonstration/Riot - Economic Catastrophe (market crash, loss of confidence)
• Natural Disaster: - High Wind (Hurricane, Tornado) - Winter Storm - Major Earthquake - Solar Weather - Drought	 - Floods - Tsunami - Volcanic Eruption - Wildfire
Process Threats and Hazards	
• Inadequate Critical Supply • Supply Chain Failure	• Poor Process Design • Single Points of Failure
Internal Threats and Hazards	
• Insider Threat • Disgruntled Employee • Failure to Make Timely Decisions • Failure to Recognize Requirements/Obstacles	• Sabotage • IT System Crash • Poor Planning • Incompetence

Multiple structured analytic techniques may be used to perform quantitative and qualitative analyses that help to determine consequences and cascading effects if MEF performance is disrupted. The extent of MEF disruption and related impacts may be characterized as:

- Severe: Extensive loss of life and property.
- Serious: Disruption to infrastructure over an extended period of time.
- Significant: Notable disruption.
- Limited: Some impact to select personnel or supporting infrastructure over a brief period of time.
- Minor: Impact to select personnel over a brief period of time.
- No impact.

Quantitative analysis aids in assessing risk based on the use of numbers where the meanings or values are established independently on a numeric scale. These numbers are arbitrary and serve to characterize impacts as part of the risk assessment.[10] A sample scale is provided in Table D-2.

Step 3a: MEF Quantitative Assessment: An organization determines the impact or consequences if failure to perform the MEF occurs (consider the worst case) and prevents or delays the performance of other essential functions. Based on the impact of failure, the organization assigns a numeric value to each MEF (reference Table D-2).

Step 3b: Resource Requirement Quantitative Assessment: An organization determines the impact or consequences if failure to meet MEF resource requirements or failure of critical assets occurs (consider the worst case) and prevents or delays the performance of the MEF. Based on the impact of failure, assign a numeric value to each MEF (reference Table D-2).

Table D-2. Sample Continuity Criticality Value Table

Quantitative Scoring Definitions	
Continuity Criticality Level 4	*Very high consequence*: Loss or disruption of the MEF, required resources, or critical assets have exceptionally grave consequences, such as extensive loss of life, widespread severe injuries, and total loss of primary mission, core functions, and processes.
Continuity Criticality Level 3	*High consequence*: Loss or disruption of the MEF, required resources, or critical assets have grave consequences, such as loss of life, severe injuries, and significant loss of primary mission, core processes, and functions for an extended period of time.
Continuity Criticality Level 2	*Medium consequence*: Loss or disruption of the MEF, required resources, or critical assets have moderate to serious consequences, such as injuries or impairment of core functions and processes.
Continuity Criticality Level 1	*Low consequence*: Loss or disruption of the MEF, required resources, or critical assets have minor consequences or impact, such as a slight impact on core functions and processes for a short period of time.

[10] U.S. Department of Homeland Security, *DHS Risk Lexicon*, 2010 Edition, September 2010, p. 25.

Qualitative analysis aids in assessing risk based on non-numerical categories or levels. Impacts may be characterized as low, medium, or high risk.[11]

Step 3c: MEF Qualitative Assessment: An organization describes the level of impact of failure to perform the MEF. This must include an explanation of the impact if the MEF is not performed. This will help articulate why the function is mission essential.

Step 3d: Resource Requirement Qualitative Assessment: An organization describes the level of the impact of failure if the MEF resource requirement or critical asset is not functioning or unavailable. This will help articulate why the resource requirement or critical asset is mission essential.

Step 4: Determine the timeframe for unacceptable loss of functions and critical assets: Organizations must analyze and determine acceptable versus unacceptable downtimes for MEFs and resource requirements identified in the BPA based on input from personnel that support those functions and have requisite experience in key areas. For example, a 12-hour delay to start processing disaster claims may be acceptable, while a 12-hour delay for initiating search and rescue missions is not acceptable.

Step 4a: Maximum Tolerable Downtime (MTD): An organization assigns an MTD to each MEF identified in the BPA. An MTD is the maximum amount of time acceptable for a disruption to or degradation of MEF performance. Consideration must be given to the impact of downtime on supporting infrastructure and activities, including the estimated duration of a resource loss before it affects the MEF it supports (see Step 4b). When evaluating impacts, organizations should also consider whether another organization may be able to perform the MEF if they cannot do so within an acceptable timeframe.

Step 4b: Recovery Time Objective (RTO): An organization assigns an RTO to each resource requirement or critical asset identified in the BPA, considering the MTDs for the function(s) it supports. An RTO is a value describing the maximum amount of time that a resource requirement or critical asset can be unavailable before it has a failure impact on essential functions. The RTO helps to ensure necessary lead time for resources required to support MEFs within their MTDs.

Describing the extent of impact of MEF failure in terms of MTDs and RTOs will support risk-informed decision making, particularly in the development and implementation of risk management options and mitigation strategies. Organizations should incorporate mitigation strategies into the organization's risk management program to sustain essential functions and the development of the organization's continuity program.

Step 5: Document the BIA: In this step, an organization documents the BIA process using the information gathered during Steps 1 – 4. Documenting the process will describe potential impacts to MEF performance and resource requirement availability and will be used to inform decision making on resource allocation to manage risks.

[11] U.S. Department of Homeland Security, *DHS Risk Lexicon*, 2010 Edition, September 2010, p. 25.

BIA documentation must include the following information:

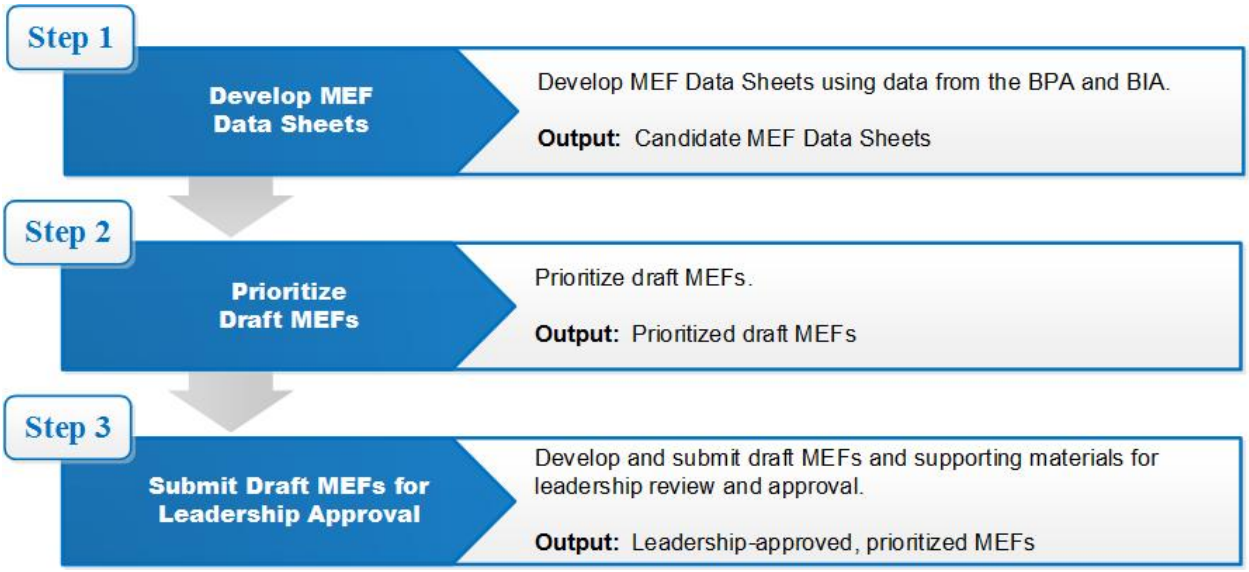
1. List of key staff, subject-matter experts, and leadership who provided input for the analysis.
2. Key findings on impacts to MEFs, resource requirements, and critical assets, summarizing results of quantitative and qualitative assessments to inform prioritization based on criticality.
3. Description of relevant threats and hazards, supporting information on likelihood of their occurrence on essential functions, and descriptions of those impacts or consequences on essential functions, referencing MTDs and RTOs.

ANNEX E: DOCUMENTATION AND PRIORITIZATION

After completing a BPA and BIA, organizations should document, prioritize, and submit updated MEFs for leadership approval. Approved and prioritized MEFs enable D/As to perform effective continuity planning and allocation of the resources required to perform MEFs under all conditions.

Figure E-1 outlines a three-step process to support the documentation, prioritization, and submission for leadership approval of draft MEFs.

Figure E-1. Documentation and Prioritization Steps



Step 1: Develop MEF Data Sheets: Organizations will complete documentation for each MEF to describe the function and analysis results using the MEF Data Sheet. The MEF Data Sheet includes the following information based on the BPA and BIA:

1. **Department/Agency:** The name of the organization responsible for performance of the MEF.
2. **MEF Statement:** A short, concise statement that briefly describes the action to be conducted and why that function is mission essential. The MEF statement is generally one sentence.
3. **MEF Narrative:** A comprehensive explanation of how the MEF facilitates the performance of an organization's mission and why that function is mission essential. The narrative may be multiple paragraphs, depending on the level of complexity of the MEF, and must describe the function so that non-experts 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 should not be included in the MEF narrative. The MEF narrative must include:

   a. The statute, regulation, presidential directive, or other legal authority requiring the conduct of the MEF.
   b. The products or services provided as a result of performing the MEF.
   c. The actions the organization must perform to accomplish the MEF.
4. **Impacts if not Conducted:** A short explanation of the impact of not performing or delaying performance of the MEF. This statement may only be a few sentences to articulate why this function is mission essential. The BIA will address the specific details of the impacts of MEF failure, so that information should not be included in the brief impact statement.
5. **Supported PMEF/NEF:** Identify the NEF with which the MEF is primarily associated, as appropriate. While some MEFs could be associated with multiple NEFs, it is important to select the single NEF that it most directly supports. If the MEF supports a PMEF (belonging to the organization or to another agency), clearly identify this linkage; see Annex F – *Primary Mission Essential Function Analysis* for additional information on PMEF determination. Not all MEFs will support a PMEF/NEF, as they may exist only to meet individual D/A mission requirements.
6. **MTD:** A statement that affirms if the MEF must be continuously performed or how quickly it must be resumed if disrupted. The MTD and related RTOs will drive continuity planning, resource, and budget considerations.
7. **Dependencies and Interdependencies:** Identify the internal and external partners and stakeholders necessary to ensure successful MEF performance and the associated dependencies and interdependencies.
8. **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 telephone number.

Organizations must use Annex G – Form 3, *Mission Essential Function Data Sheet Template*, to document this MEF data and retain all supporting documentation.

Step 2: Review and Prioritize MEFs: Organizations must prioritize MEFs based upon structured analysis supported by the information gathered during the BPA and BIA processes. Prioritizing MEFs will support the development of continuity plans and identification of resource requirements for MEF performance.

Organizations must consider several factors when prioritizng MEFs:

1. **Impacts if not Conducted:** The impacts of not conducting or delaying the performance of each MEF most informs determination of priorities. The more severe the impact, the higher priority the MEF.
2. **MTD:** The MTD assigned to each MEF during the BIA process will define the maximum amount of time acceptable for a disruption or degradation to MEF performance.
3. **RTO:** The RTO identified during the BIA process will define the maximum amount of time the resource requirement or critical asset may be unavailable before having an adverse impact on the performance of essential functions. MEFs that must be continuously performed and those with the shortest recovery times will generally be given priority.
4. **Leadership Priority:** Some MEFs will have a higher priority due to leadership direction.

Step 3: 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 package will vary based on individual D/A requirements. The package should include prioritized MEFs and appropriate supporting material to enable an informed decision from leadership on MEF prioritization and whether each function should be categorized as a MEF rather than an ESA.

ANNEX F: PRIMARY MISSION ESSENTIAL FUNCTION ANALYSIS

After organizations have completed the process of identifying and validating their MEFs, they must analyze each MEF to determine if it supports continual performance of the NEFs and, therefore, should be considered as a candidate PMEF. Organizations must also review and validate existing PMEFs and identify any changes based on performance requirements.

D/As must biennially review their MEFs and PMEFs to determine if a PMEF continues to supports the NEFs.

Candidate PMEF Identification and Analysis: D/As must determine if a MEF, 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 that the MEF or candidate PMEF function must be continuously performed to support or implement the uninterrupted performance of NEFs.

D/As must document the candidate PMEF by completing Annex G – Form 4, *Candidate PMEF Data Worksheet*.

Candidate PMEF Submission: The National Continuity Coordinator (NCC) will establish an IAB working group to review and recommend candidate PMEFs submitted by organizations prior to submission to the NCC for final approval. Candidate PMEFs are reviewed by the IAB to ensure a consistent standard is applied across the Federal Executive Branch in the determination of approved PMEFs.

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

1. **Agency Memorandum:** A memorandum from the D/A Continuity Coordinator 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 Manager for IAB coordination.
2. **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, narrative description, impact statement concerning PMEF failure, identification of the supported NEF, MTD, dependencies and interdependencies, and point of contact.
3. **BPA and BIA Documentation:** Organizations must submit copies of BPA and BIA reports and other appropriate documentation supporting the candidate PMEF.

IAB Process: An IAB will conduct a joint review of submitted candidate PMEFs with each D/A Continuity Coordinator to evaluate the relationship of each PMEF to the NEFs.

The IAB will conduct:

1. An analysis of Federal Executive Branch PMEF interdependencies for each NEF to more accurately depict PMEF execution capability.
2. A BPA to identify and map interagency PMEF processes and resources required for the performance of each NEF. The BPA will define how each NEF is executed by determining business process flows with the NEF serving as the "output" and PMEFs serving as the "inputs."
3. NEF-specific BIAs to:
    a. Identify potential single points of failure and risks that may adversely affect the execution of interagency PMEF support to NEFs.
    b. Identify the impact of disruption to performance of interagency PMEFs.
    c. Identify potential PMEF process alternatives to minimize disruption to NEF performance.

The IAB will submit recommended PMEFs and supporting documentation to the NCC for review and approval.

ANNEX G: FORMS

This Annex provides worksheets and templates to assist organizations with identifying, reviewing, and validating MEFs and candidate PMEFs and to assist with documenting key elements of a BPA and BIA. Each form correlates to guidance and processes outlined in this FCD.

The following forms are provided:

- Form 1: Organizational Functions Worksheet
- Form 2: Business Process Analysis Data Sheet Template
- Form 3: Mission Essential Function Data Sheet Template
- Form 4: Candidate PMEF Data Worksheet

Form 1. Organizational Functions Worksheet

Function	Requirement to Perform Function	Products or Services of Function	Essential (X)	Non-Essential (X)	Mission Essential Function (X)	Essential Supporting Activity (X)

Form 2. Business Process Analysis Data Sheet Template

Business Process Analysis Data Sheet
MEF Statement:
MEF Description:
MEF Outputs:
MEF Inputs:
Dependencies and Interdependencies:
Leadership:
Staff:
Communications and Information Systems:
Facilities:
Resources and Budgeting:
Process Details:
Other Comments:

Form 3. Mission Essential Function Data Sheet Template

MEF Data Sheet Date: _____
Department/Agency:
MEF Statement:
MEF Narrative:
Impacts if not Conducted:
Supported PMEF/NEF:
MTD:
Dependencies and Interdependencies:
Point of Contact:

Form 4. Candidate Primary Mission Essential Function Data Worksheet

Candidate PMEF Data Worksheet Date: _____
Department/Agency:
Candidate PMEF Statement:
Candidate PMEF Narrative:
Impacts if not Conducted:
Supported NEF(s):
MTD:
Dependencies and Interdependencies:
Point of Contact:

ANNEX H: ACRONYMS

BIA	Business Impact Analysis
BPA	Business Process Analysis
COG	Continuity of Government
COOP	Continuity of Operations
D/A	Department and Agency
ECG	Enduring Constitutional Government
ESA	Essential Supporting Activity
FEMA	Federal Emergency Management Agency
HQ	Headquarters
IAB	Interagency Board
MEF	Mission Essential Function
MTD	Maximum Tolerable Downtime
NCC	National Continuity Coordinator
NCP	National Continuity Programs
NEF	National Essential Function
PMEF	Primary Mission Essential Function
PPD	Presidential Policy Directive
SOP	Standard Operating Procedure

ANNEX I: DEFINITIONS

Catastrophic Emergency – Any event, regardless of location, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the U.S. population, infrastructure, environmental, economy, or government functions.[12]

Essential Functions – Subsets of government functions that are categorized as Mission Essential Functions (MEFs), Primary Mission Essential Functions (PMEFs), and National Essential Functions (NEFs).[13]

Essential Supporting Activities (ESAs) – Functions that support performance of MEFs but do not reach the threshold of MEFs or PMEFs. ESAs are important facilitating activities performed by most organizations (e.g., providing a secure workplace, ensuring computer systems are operating); however, the sole performance of ESAs does not directly accomplish an organization's mission.[14]

Government Functions – The collective functions of the Executive Office of the President and D/As, as defined by statute, regulation, presidential directive, or other legal authority, and the functions of the legislative branch and judicial branch.[15]

Interagency Board (IAB) – A working group established by the NCC to review and recommend candidate PMEFs submitted by organizations before submission to the NCC for final approval.

Mission Essential Functions (MEFs) – Essential functions directly related to accomplishing the organization's mission as set forth in statutory or executive charter. Generally, MEFs are unique to each organization.[15]

National Essential Functions (NEFs) – Select functions that are necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through COOP, COG, and ECG capabilities.[15]

Primary Mission Essential Functions (PMEFs) – Those MEFs that must be continuously performed to support or implement the uninterrupted performance of NEFs.[15]

[12] PPD-40, p. 1.
[13] PPD-40, p. 2.
[14] FCD-1, p. B-1.
[15] PPD-40, p. 3.

ANNEX J: AUTHORITIES AND RESOURCES

AUTHORITIES:

1) Homeland Security Act of 2002, as amended (6 U.S.C. § 101 et seq.).
2) The National Security Act of 1947, as amended (50 U.S.C. § 3042).
3) USA Patriot Act of 2001, October 6, 2001.
4) Executive Order 12148, *Federal Emergency Management*, July 20, 1979, as amended.
5) Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities*, November 18, 1988, as amended.
6) Executive Order 13286, *Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security*, February 28, 2003.
7) Presidential Policy Directive 8, *National Preparedness*, March 30, 2011.
8) Executive Order 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, July 6, 2012.
9) Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, February 12, 2013.
10) Presidential Policy Directive 40, *National Continuity Policy*, July 15, 2016.
11) Office of Science and Technology Policy/Office of Management and Budget D-16-1 *Minimum Requirements for Federal Executive Branch Continuity Communications Capabilities*, December 16, 2016.

RESOURCES:

1) 36 Code of Federal Regulations, Part 1223, *Managing Vital Records*.
2) 44 Code of Federal Regulations, Part 3541, *Federal Information Security Management Act of 2002*.
3) Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements*, January 17, 2017.
4) National Incident Management System, November 2016.
5) National Preparedness Goal, September 2015.
6) National Institute of Standards and Technology, Special Publication 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.
7) National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Recommended Security Controls for Federal Systems and Organizations*, August 2013.
8) 1600 Standard on Disaster/Emergency Management and Business Continuity Programs, National Fire Protection Agency, 2013 Edition.
9) *National Infrastructure Protection Plan (NIPP)*, U.S. Department of Homeland Security, 2013.
10) NIPP Supplemental Tool: *Executing a Critical Infrastructure Risk Management Approach.*
11) National Institute of Standards and Technology, Special Publication 800-30, Rev 1, *Guide for Conducting Risk Assessments*, September 2012.

12) National Institute of Standards and Technology, Special Publication 800-39, *Managing Information Security Risk Organization, Mission, and Information System View*, March 2011.
13) *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*, August 2013, 1st Edition.
14) *DHS Risk Lexicon*, 2010 Edition, U.S. Department of Homeland Security, September 2010.