U.S. Department of Homeland Security
Federal Emergency Management Agency
Federal Continuity Directive 1
Issue Date: January 17, 2017

Federal Continuity Directive 1

Federal Executive Branch National Continuity Program and Requirements

Table of Contents

I. Purpose 3

II. Scope 3

III. Supersession 3

IV. Policy and Background 3

V. Roles and Responsibilities 5

VI. Federal Executive Level Continuity Coordination Meetings 5

VII. Continuity Capability Elements 6

VIII. Readiness Reporting System 9

IX. Continuity Operational Phases and Implementation 9

X. Coordination with State, Local, Tribal, and Territorial Governments, Non-Governmental Organizations, and Private Sector Critical Infrastructure Owners and Operators 9

XI. Operations Security 10

XII. Point of Contact 10

XIII. Distribution 11

ANNEX A: PROGRAM MANAGEMENT, PLANS, AND PROCEDURES A-1

ANNEX B: ESSENTIAL FUNCTIONS B-1

ANNEX C: ORDERS OF SUCCESSION C-1

ANNEX D: DELEGATIONS OF AUTHORITY D-1

ANNEX E: COMMUNICATIONS AND INFORMATION SYSTEMS E-1

ANNEX F: ESSENTIAL RECORDS MANAGEMENT F-1

ANNEX G: ALTERNATE LOCATIONS G-1

ANNEX H: HUMAN RESOURCES H-1

ANNEX I: DEVOLUTION I-1

ANNEX J: RECONSTITUTION J-1

ANNEX K: TEST, TRAINING, AND EXERCISE PROGRAM K-1

ANNEX L: CONTINUITY OPERATIONAL PHASES AND IMPLEMENTATION L-1

ANNEX M: ACRONYMS M-1

ANNEX N: DEFINITIONS N-1

ANNEX O: AUTHORITIES AND RESOURCES O-1

I. Purpose

Presidential Policy Directive 40 (PPD-40), *National Continuity Policy*, directs the Secretary of Homeland Security through the Administrator of the Federal Emergency Management Agency (FEMA) to coordinate the implementation, execution, and assessment of continuity activities among executive departments and agencies (D/As). Specifically, the Administrator of FEMA is directed to *develop and promulgate Federal Continuity Directives to establish continuity program and planning requirements for executive departments and agencies.* This Federal Continuity Directive 1 (FCD-1) implements this requirement by establishing the framework, requirements, and processes to support the development of D/As' continuity programs and by specifying and defining elements of a continuity plan. These required elements include delineation of essential functions; succession to office and delegations of authority; safekeeping of and access to essential records; continuity locations; continuity communications; human resources planning; devolution of essential functions; reconstitution; and program validation through testing, training, and exercises (TT&E).

II. Scope

In accordance with PPD-40, the provisions of this FCD apply to the 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 Executive Branch. The provisions of this FCD are applicable at all levels of Executive Branch organizations regardless of their location, including regional and field locations. Headquarters (HQ) elements are responsible for providing oversight and promulgating this directive to their subcomponent and field organizations. In this FCD, the term "*headquarters*" refers to the central, head offices of operations for organizations identified in PPD-40, Annex A, *Categories of Departments and Agencies*. The terms "*component*" or "*subcomponent*" refer to all organizational elements, whether at headquarters or a regional or field office.

III. Supersession

This FCD rescinds and supersedes FCD-1, F*ederal Executive Branch Continuity Program and Requirements*, February 2012.

IV. Policy and Background

A. <u>Policy</u>: As established in PPD-40, "it is 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 resilience and preservation of government structure under the United States Constitution and the continuous performance of National Essential Functions (NEFs) under all conditions." National continuity programs are based on the continuous performance of NEFs through the sustainment of essential functions performed by D/As. NEFs are the focal point 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. The NEFs are:

1) Ensuring the continued functioning of our form of government under the United States Constitution, including the functioning of three separate branches of government;
2) Providing leadership visible to the Nation and the world and maintaining the trust and confidence of the American people;
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 interests;
4) Maintaining and fostering effective relationships with foreign nations;
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;
6) Providing rapid and effective response to and recovery from the domestic consequences of an attack or other incident;
7) Protecting and stabilizing the Nation's economy and ensuring public confidence in its financial systems; and,
8) Providing for Federal Government services that address the national health, safety, and welfare needs of the United States.

B. Background: On May 4, 2007, the President signed National Security Presidential Directive (NSPD)-51/Homeland Security Presidential Directive (HSPD)-20, *National Continuity Policy*, to establish a comprehensive national policy for the continuity of Federal Government structures and operations, a single National Continuity Coordinator responsible for coordinating the development and implementation of Federal continuity policies, and the National Essential Functions. In conjunction with NSPD-51/HSPD-20, the White House published the National Continuity Policy Implementation Plan (NCPIP), which provided greater detail on how D/As were to accomplish the requirements of the policy. In 2008, as directed in the policy, DHS published FCD-1 to establish continuity planning requirements for D/As. FCD-1 was updated in 2012.

On July 15, 2016, the President signed PPD-40, *National Continuity Policy*, which replacedNSPD-51/HSPD-20 and the NCPIP, addressing lessons learned, best practices, and the integration of new technologies and processes since 2007. Some relevant material in the NCPIP was added to PPD-40 and certain portions were adopted in this FCD.

Proper implementation of PPD-40 will ensure that essential functions are sustained in an all-hazards environment. The complexity of this environment increases the need for comprehensive continuity programs that emphasize agility and flexibility to sustain essential functions across a broad spectrum of conditions.

Organizations must fully integrate continuity planning and procedures into all aspects of daily operations to create a "culture of continuity". Only with a coordinated approach to

continuity can organizations effectively respond to and recover from catastrophic emergencies.

This new FCD-1 establishes minimum continuity standards for D/As to incorporate into their daily operations to ensure seamless and immediate continuation of essential functions. All Federal Executive Branch D/As, regardless of their size or location, shall have a viable continuity capability, based on the requirements and principles outlined herein, to ensure resiliency and continued performance of their organizations' essential functions under all conditions.

V. Roles and Responsibilities

PPD-40 requires appointment of a Continuity Coordinator at the Assistant Secretary level or higher. As a recommended best practice, D/As should consider appointing a Continuity Manager to handle day-to-day management of the continuity program. These roles are further explained below, but D/As should feel free to designate other positions, as desired, to assist in coordinating the implementation, execution, and evaluation of continuity plans and programs within an organization and to ensure that programs address the entirety of essential functions rather than limit scope to only headquarters:

A. <u>Continuity Coordinator</u>: The senior D/A official responsible for coordinating with the Organization Head and national continuity leadership to ensure the organization maintains a viable and effective continuity capability. The Continuity Coordinator represents the D/A on the Continuity Advisory Group (CAG) and works with other D/A heads to complete the Mission Essential Function (MEF) and Primary Mission Essential Function (PMEF) identification process, and advocates for the continuity program within the organization. The Continuity Coordinator is also responsible for validating Readiness Reporting System (RRS) reports on behalf of the organization to FEMA.

B. <u>Continuity Program Manager (Continuity Manager)</u>: On behalf of the Continuity Coordinator, Continuity Managers oversee day-to-day continuity programs and represent their D/As at inter-agency forums and working groups including the Interagency Continuity Working Group (ICWG) as appropriate. The Continuity Manager serves as the primary point of contact (POC) with the FEMA National Continuity Programs Directorate (NCP) for D/A continuity program matters, including preparedness and operational activities. The Continuity Manager administers support to components to ensure that D/A leadership and continuity personnel are properly trained and facilities properly equipped to execute continuity plans with little or no notice.

VI. Federal Executive Level Continuity Coordination Meetings

Federal executive level continuity coordination meetings are designed to serve as executive-level forums for promoting the development, coordination, and integration of continuity planning and programs within the Executive Branch. Continuity Managers and other continuity POCs work collaboratively to plan and coordinate implementation of the *National Continuity Policy* within their respective organizations.

A. <u>Continuity Advisory Group (CAG)</u>: FEMA NCP representatives chair this inter-agency forum focused on the implementation of continuity policy and programs. As the CAG Chair, and a member of the Domestic Resilience Group (DRG), FEMA will

introduce continuity policy concerns identified by the CAG to the DRG for consideration and resolution as appropriate. The CAG is comprised of Continuity Coordinators, or their designees, from Category I, II, III, and IV organizations. State, local, tribal, and territorial (SLTT) government representatives from the National Capital Region (NCR) and representatives from the legislative and judicial branches may also participate, as appropriate.

B. Interagency Continuity Working Group (ICWG): FEMA NCP chairs this forum comprised of Federal Continuity Managers and continuity planners. The ICWG meets regularly to provide a forum for Continuity Program Managers to coordinate a collaborative strategy for the implementation of the *National Continuity Policy* and Federal Continuity Directives. The ICWG promotes improved federal continuity standards, practices, and procedures, and is specifically intended to enhance continuity planning, training, and exercises; emergency management; and resiliency capabilities for executive branch organizations.

C. Small Agency Council Continuity of Operations Committee (SAC COOPC): A forum for the implementation of continuity policy and development and integration of continuity programs among Category IV organizations. FEMA assists the SAC COOPC on continuity preparedness matters as requested by the SAC COOPC Chair.

VII. Continuity Capability Elements

PPD-40 outlines the overarching continuity requirements for organizations. The consideration, preparation, and execution of the continuity elements listed in this section are fundamental to a successful continuity program. Continuity Managers and continuity planners must coordinate with the offices of Chief Information Officers, Chief Human Capital Officers, General Counsels, Chief Financial Officers, and others to provide specialized subject-matter expertise to enhance the organization's continuity program planning and implementation.

Annual requirements of this FCD are defined as those scheduled to occur during the federal fiscal year, October 1 through September 30. Required continuity elements are as follows:

A. Program Management, Plans, and Procedures: Establishment of continuity program planning objectives and procedural requirements are critical to sustainment of essential functions during a continuity activation. Alignment of resources to continuity plans and procedures is critical to ensure execution and to sustain essential functions through all phases of activation. The application of risk management principles can preserve resources by assessing the probability of occurrence for catastrophic emergencies and related consequences. *See Annex A – Program Management, Plans and Procedures for specific requirements.*

B. Essential Functions: Sustainment of the NEFs in an all-hazards environment requires federal organizations to identify MEFs and PMEFs, and to establish programs to ensure continuity of those functions throughout, or to resume them rapidly, during a disruption to normal operations. The identification and prioritization of essential functions is the foundation of continuity planning, and establishes the parameters that drive an organization's continuity planning and preparedness efforts. When MEFs are performed outside the National Capital Region (NCR), organizations must implement procedures for assessing and reporting the ability to sustain essential functions when regional and field

offices are affected by catastrophic emergencies that occur in their areas. *See Annex B – Essential Functions for specific requirements.*

C. **Orders of Succession:** Orders of succession ensure that an organization has identified key personnel to assume leadership positions in the event that regularly appointed personnel are unavailable. Those identified in the orders of succession must be trained annually on responsibilities and shall participate in TT&E events. *See Annex C – Orders of Succession for specific requirements.*

D. **Delegations of Authority:** Clearly established delegations of authority are essential to ensure that continuity personnel have the appropriate legal authority to make key decisions and take action during catastrophic emergencies. Delegations of authority are activated when normal operational conditions are disrupted, and are deactivated once the organization determines that the disruption has ended and normal operations can be resumed. Organizations establish delegations of authority in advance to ensure the orderly transition of leadership responsibilities during a continuity activation. *See Annex D – Delegations of Authority for specific requirements.*

E. **Communications and Information Systems:** Availability, diversity, and redundancy of critical communications and information systems are critical to sustain essential functions performed at primary and alternate locations including devolution locations as well as telework or mobile work environments. Communications and information systems provide the connectivity between and among key government leadership, internal elements, other organizations, and the public to perform essential functions. Telework and mobile work environments require use of portable telecommunications technology such as laptop computers, mobile telephones, and satellite communications equipment. *See Annex E – Communications and Information Systems for specific requirements.*

F. **Essential Records Management:** Viable continuity programs include comprehensive processes for identification, protection, and accessibility of electronic and hardcopy essential records at primary, alternate, and devolution locations. Essential records may include documents, references, personnel records, and information systems. Redundant data management software applications and equipment should be standardized throughout the organization, and must provide the appropriate level of access and cybersecurity to protect classified, sensitive, and personally identifiable information. Official access rosters must be carefully managed and maintained, and primary and alternate essential records management personnel must be identified to ensure access to essential information at all locations, under all conditions. *See Annex F – Essential Records Management for specific requirements.*

G. **Alternate Locations:** Alternate locations are where essential functions are continued or resumed, or where organizational command and control may occur during a continuity event. An alternate location should be chosen based on risks identified during the Business Impact Analysis process and should be located with sufficient geographical distance from the organization's primary facility. Alternate locations may be intended to support deployed Emergency Relocation Group (ERG) members who perform continuity operations, or may only support deployment of the Organization Head (or successor) and a small continuity team. A devolution site is located outside the primary region, and is

capable of assuming the statutory and legal authority and responsibilities of the primary operating staff and facilities to sustain essential functions when necessary.

Telework, mobile work, and work performed from directed work locations may be leveraged to support continuity operations. Mobile work refers to tasks performed while employees travel from one work location to another. Directed work locations refer to occasions when employees are directed to perform assigned duties at locations other than at designated work locations, which may include private residence, satellite offices, and alternate locations. Telework is a program that can provide critical support to the sustainment of 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. *See Annex G – Alternate Locations for specific requirements.*

H. Human Resources: Organizations must identify continuity personnel, consisting of leadership, staff, and functional support elements capable of relocating to alternate locations or assuming devolved functions. During continuity activation, organizations will mobilize designated personnel as needed to sustain essential functions in accordance with approved continuity plans and procedures. Viable continuity programs include procedures to sustain administrative services, personnel accountability, and support services to employees not identified as continuity personnel, and are likely to be affected by a catastrophic emergency. *See Annex H – Human Resources for specific requirements.*

I. Devolution: Devolution is a component of continuity planning that establishes procedures to transfer statutory authority and responsibilities from an organization's primary operating staff and facilities to another designated staff and one or more facilities for the purpose of sustaining essential functions. Devolution may be temporary, or may endure for an extended period. A devolution plan is activated upon the threat of, or in response to a catastrophic emergency that either renders the organization's primary leadership and operating staff unavailable, or leaves them incapable of sustaining essential functions from primary facilities. *See Annex I – Devolution for specific requirements.*

J. Reconstitution: Reconstitution is the final phase of a continuity event, and is the process by which surviving and/or replacement personnel resume normal operations and may occur at any designated location that provides the staff, facilities, and systems necessary to sustain essential functions. *See Annex J – Reconstitution for specific requirements.*

K. Test, Training, and Exercises: Test, training, and exercise (TT&E) events assess and validate continuity plans, policies, procedures, systems, and alternate locations. Initial and recurring training programs inform and familiarize leaders and staff with continuity plans and procedures. Exercise programs consisting of both planned and short/no-notice events improve an organization's preparedness posture, and emphasize the value of integrating continuity functions into daily operations. The corrective actions identified during individual exercises are tracked to completion, ensuring that exercises yield tangible preparedness improvements. An effective corrective action program develops improvement plans that are dynamic documents, which are continually monitored and implemented as part of the larger system of improving preparedness. All organizations

must incorporate a TT&E strategy into continuity programs. *See Annex K – Test, Training, and Exercises for specific requirements.*

VIII. Readiness Reporting System

The Readiness Reporting System (RRS) is an automated system FEMA maintains to track federal continuity capabilities at all times under all conditions. RRS provides a method for Executive Branch organizations to report their capacity to perform MEFs and PMEFs. FEMA provides information obtained from RRS to inform the National Continuity Coordinator on comprehensive Executive Branch continuity capability.

Organizations are required to submit Continuity Status Reports (CSRs) and performance data via the RRS each month, during continuity events, or as otherwise directed. Continuity Managers coordinate RRS system access requirements and operator training with FEMA NCP. *See Annex L – Operational Phases and Implementation for RRS reporting requirements during various phases of continuity operations.*

IX. Continuity Operational Phases and Implementation

There are four phases of continuity operations: readiness and preparedness, activation, continuity operations, and reconstitution. These four phases should be used to build continuity processes and procedures, establish goals and objectives, and support the performance of organizational PMEFs/MEFs during a catastrophic emergency. *See Annex L – Continuity Operational Phases and Implementation.*

X. Coordination with State, Local, Tribal, and Territorial Governments, Non-Governmental Organizations, and Private Sector Critical Infrastructure Owners and Operators

Continuity of Government and sustainment of the NEFs requires the integration of executive, legislative, and judicial programs that are coordinated across all levels of government, Non-Governmental Organizations (NGOs), and critical infrastructure sectors. Government offices at the SLTT levels are critical to serving the public through delivery of essential services during catastrophic emergencies. The resilience of SLTT governments enhances the effectiveness of federal response and recovery operations, and provides visible leadership.

FEMA will integrate continuity and resiliency requirements or incentives into future FEMA SLTT grant guidance to encourage jurisdictions to develop viable continuity plans to ensure the performance of essential functions and sustain the delivery of essential services and core capabilities across all hazards.

Federal organizations, as applicable, will coordinate with SLTT governments, regional entities, and critical infrastructure sectors to promote integration and collaboration. Such partnerships improve resilience and enhance unity of effort. Examples of coordination activities that federal organizations may undertake include:

1. Collaboration to incorporate capabilities of other entities into the organization's continuity planning and exercise activities;

2. Coordination of risk assessments to identify threats and hazards relevant to the organization's mission and the location(s) where essential functions are performed;
3. Partnering to coordinate continuity plans;
4. Participation in Continuity Working Groups (CWGs), information sharing, training, and exercises, as appropriate;
5. Coordination of occupant emergency, shelter-in-place, and regional and local evacuation plans;
6. Participation in existing alert and notification networks and credentialing initiatives;
7. Collaboration to identify interdependencies and ensure critical infrastructure resilience at all levels;
8. Coordination of continuity resources and security requirements, as appropriate;
9. Augmentation and participation in coordination activities to include, but not limited to those of: DHS/FEMA Regional/State-level CWGs, DHS/Office of Infrastructure Protection, Critical Infrastructure Sector Coordinating Councils and Government Coordinating Councils, Information Sharing and Analysis Centers; and,
10. Participation in other coordination activities, as appropriate.

FEMA NCP and the 10 FEMA Regional Headquarters located throughout the country conduct regional and state-level CWGs, and host annual continuity conferences to promote and assist in integrating federal and SLTT continuity planning. FEMA NCP training courses to support development of continuity programs at SLTT levels, and within critical infrastructure sectors are also available through the Emergency Management Institute.

XI. Operations Security

Operations Security (OPSEC), Information Security (INFOSEC), Cyber Security, and other efforts are applied to protect against an evolved threat environment targeting federal and SLTT agencies and critical infrastructure continuity plans and programs. Organizations must implement comprehensive multi-disciplinary security actions such as identification of essential elements of information; risk analysis; and application of appropriate physical, communications, information, and personnel security measures and countermeasures to protect continuity plans, programs, alternate locations, networks, and personnel against hostile actions.

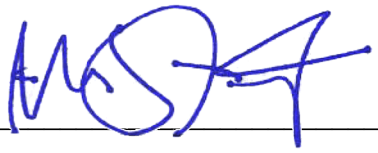
Organizations shall report threats, events, and/or suspicious activity directed against continuity programs to the U.S. Department of Homeland Security within 12 hours of its occurrence or discovery, as conditions warrant, through normal suspicious activity reporting protocols.

XII. Point of Contact

Please contact the Assistant Administrator, NCP, FEMA, for assistance with the information contained in this FCD at (202) 646-4145 or email at FEMA-NationalContinuity@fema.dhs.gov.

XIII. 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.



January17, 2017

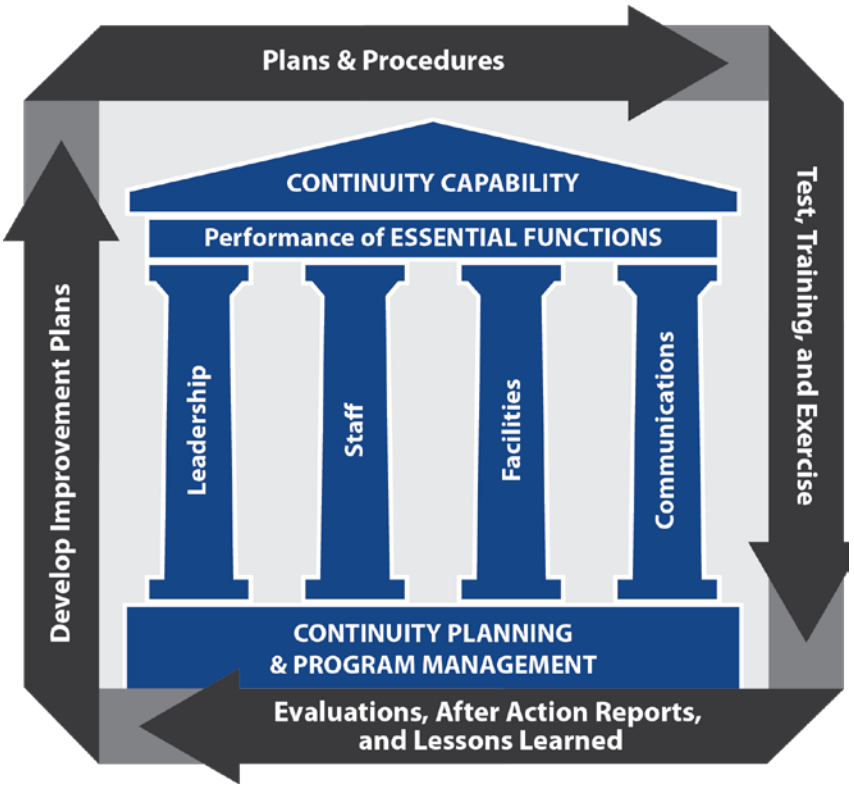
W. CRAIG FUGATE
Administrator, FEMA

Date

ANNEX A: PROGRAM MANAGEMENT, PLANS, AND PROCEDURES

A standardized continuity program management cycle provides consistency across Federal Government continuity programs. Establishment of standardized planning and procedural objectives and requirements ensures sustainment of essential functions during a catastrophic emergency. Use of the Continuity Program Management Cycle facilitates development and implementation of resilient continuity programs. See Figure A-1, Continuity Program Management Cycle.

Figure A-1. Continuity Program Management Cycle



A Multi-Year Strategy and Program Management Plan (MYSPMP) provides planning guidance for the development of effective continuity programs that support the organization's continuity mission. The MYSPMP serves as a roadmap for organizations to ensure that continuous activities and resources are acquired to sustain the program and support continuous improvement efforts.

Organization leaders must apply sufficient resources to support continuity program requirements and the program objectives must:

1. Ensure the organization can sustain essential functions throughout any emergency;
2. Reduce loss of life and mitigate threats to property;
3. Incorporate risk management principles across the program, including identification and assessment of potential threats and hazards and their associated impacts; acceptable risk determination; and identification of required mitigation resources;

4. Establish statutory orders of succession and delegations of authority to ensure sequential assumption of legal authorities and responsibilities by holders of other specified positions within the organization;
5. Reduce or mitigate operational disruptions;
6. Identify, maintain, and operate alternate locations from which organizations can perform essential functions;
7. Protect personnel, alternate locations, equipment, records, and other assets critical to the performance of essential functions;
8. Provide for timely and orderly recovery and reconstitution;
9. Dedicate the resources required to sustain essential functions; and,
10. Establish a realistic and challenging test, training, and exercise program to verify continuity capabilities.

Risk analysis encapsulates information on what may go wrong (risk assessment) and on what can be done to lessen the occurrence of certain threats/hazards or mitigate their consequences (risk management). Risk management is a comprehensive process that requires organizations to identify, analyze, assess, and prioritize risk. Organizations may then accept the risk or apply resources to mitigate or control its impacts. The key to an effective risk management program is understanding potential risks and the organization's relation to those risks. Organizations conduct and document a risk assessment of all MEFs by completing a Business Impact Analysis (BIA) for all threats and hazards, and all capabilities associated with the continuance of essential functions at least every two years. FCD-2, *Federal Executive Branch Mission Essential Function and Candidate Primary Mission Essential Function Identification and Submission Process*, contains additional guidance and direction on BIAs and supplemental information may further assist in risk analysis.

REQUIREMENTS AND CRITERIA FOR PROGRAM MANAGEMENT, PLANS, AND PROCEDURES:

1. Continuity programs must address all elements of continuity: program management, plans, and procedures; essential functions; orders of succession; delegations of authority; communications and information systems; essential records management; alternate locations; human resources; devolution; reconstitution; test, training, and exercises; and, the four phases of continuity: (1) readiness and preparedness, (2) activation, (3) continuity operations, and (4) reconstitution. They must also address the requirements associated with each element contained in this FCD. These elements include:
    a. A continuity plan approved and signed by the Organization Head, such as the Secretary, Director, Administrator, or designee.
    b. A review of the organization's continuity plan annually and updated as required. The date of the review and the names of personnel conducting the review must be recorded.
    c. Implementation of a process for determining an organization's readiness posture and continuity decision-making protocols to increase readiness. Organizations

must establish internal procedures for executing changes to the Continuity of Government Readiness Conditions (COGCON), as appropriate.

d. Implementation of a process or methodology that ensures the implementation of a continuity plan including a decision matrix for activation with warning and without warning during duty and non-duty hours.

e. Implementation of a process or methodology to ensure operations can be sustained for a minimum of 30 days following a catastrophic emergency or until normal operations are resumed. This includes planning for the challenges posed by continuity events that extend past 30 days.

f. Establishment and maintenance of appropriate relocation procedures and instructions for Emergency Relocation Group (ERG) and Devolution Emergency Response Group (DERG) members to support continuity and devolution at alternate locations.

   a. Detail processes and procedures for activating alternate locations.

   b. Detail the transition of responsibilities to the deployed ERG and DERG.

2. Continuity plans require a process for attaining capabilities at alternate locations as soon as possible but no later than 12 hours following the activation of continuity plans for D/As with MEFs and must be continuously performed for D/As with PMEFs. Such plans must include:

   a. Triggers for plan activation.

   b. A process for attaining and reporting D/A operational capability reflecting the status of headquarters and other facilities, such as regional or field offices, where PMEFs and MEF are performed.

3. Conduct and document a comprehensive risk assessment that considers all continuity capabilities and operations associated with program plans and procedures to include budgeting and acquisition; orders of succession; delegations of authority; primary and alternate locations; continuity communications; essential records; human resources; test, training, and exercise; devolution; reconstitution; and continuity operations and implementation. All risk assessments and related risk management activities must include:

   a. Identification of potential known risks and the likelihood of their occurrence;

   b. Assessment of the vulnerability of the organization's continuity capabilities and operations to identified threats and hazards;

   c. Assessment of the potential impact caused by identified threats and hazards;

   d. Determination of appropriate mitigation and countermeasures.

   e. A cost-benefit analysis of risk mitigation, management, and control measures;

   f. A plan to implement mitigation, management, or control measures during catastrophic emergencies, to include during a pandemic; and,

g. Signature of Acknowledgement by the Continuity Manager, Continuity Coordinator, or by an organization's senior executive.

4. Create a MYSPMP that provides for the development, maintenance, and annual review of continuity capabilities including at a minimum:
    a. Short- and long-term planning goals and objectives;
    b. Potential program implementation issues, concerns, and obstacles and a strategy to address each; and
    c. Planning, training, and exercise milestones and activities.
5. Fund requirements of the continuity program at all levels including regional, field, and satellite offices, including, at a minimum:
    a. Identify resources -- equipment, supplies, and personnel --necessary to sustain operations at alternate locations for a minimum of 30 days or until normal operations are resumed;
    b. Establish procedures for emergency procurement of equipment, supplies, services, and personnel to support continuity operations;
    c. Integrate continuity requirements into existing and future contracts and Memoranda of Understanding/Memoranda of Agreements (MOUs/MOAs) as applicable to ensure the continuation of essential functions during a continuity event for a minimum of 30 days or until normal operations are resumed; and,
    d. Integrate continuity programs into strategic plan objectives, performance metrics, and funding.
6. Non-HQ organization entities including subcomponent, regional, and field offices, must submit the following documentation to their organization HQ annually to provide visibility on continuity efforts at all levels of the organization:
    a. Certification that the component/office maintains a continuity plan and the date of signature. Organizations may use regional or overarching continuity/devolution plans that integrate the continuity capabilities of multiple subordinate organizations; and,
    b. Certification that the component/office participates in an annual exercise that incorporates the deliberate and preplanned movement of continuity personnel to an alternate location and the date of last exercise.
7. Organization HQ must track component's continuity plans and continuity exercise status annually.
8. Organization HQ must submit monthly continuity readiness status information via RRS no later than the 25th of each month, unless otherwise indicated by FEMA NCP. If the 25th falls on a holiday or weekend, the report must be submitted the previous business day.

ANNEX B: ESSENTIAL FUNCTIONS

The identification and prioritization of essential functions and critical assets provide the foundation of continuity planning. Continuity planning provides the framework that accounts for all continuity capabilities required in the performance of essential functions. Essential functions are critical activities used to identify key assets, supporting tasks, and resources that must be included in an organization's continuity planning process. Establishing priorities and allocating resources based on Business Process Analyses (BPAs) and BIAs ensures delivery of essential functions and serves as a mechanism for resuming functions should resources become available. FCD-2, *Federal Executive Branch Mission Essential Function and Candidate Primary Mission Essential Function Identification and Submission Process*, provides detailed guidance to assist with the identification, prioritization, and resourcing of essential functions.

Government functions are 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. Essential functions are subsets of those government functions categorized as Mission Essential Functions (MEFs), Primary Mission Essential Functions (PMEFs), and National Essential Functions (NEFs).

1. 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.
2. PMEFs are those mission essential functions that must be continuously performed to support or implement the uninterrupted performance of NEFs.
3. NEFs are select functions that are necessary to lead and sustain the Nation during a catastrophic emergency and, therefore, must be supported through COOP, COG, and ECG capabilities.

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

REQUIREMENTS AND CRITERIA FOR ESSENTIAL FUNCTIONS:

1. Review essential functions and BPAs biennially. The review must:
    a. Incorporate any identified changes generated by new programs, functions, or by changes to existing programs or functions;
    b. Reflect the date of the review and names of personnel conducting the review; and,
    c. Be submitted to the Interagency Board, through FEMA, for approval, as requested, for PMEF submissions.
2. Using the methodology outlined in FCD-2, organizations must identify, prioritize, and document essential functions in the continuity plan. These activities include:
    a. A review of functions to determine those directed by applicable laws, presidential directives, executive orders, and other policies or directives;

b. Identification of essential functions that directly support an essential function performed by another organization including when and where support is provided;

c. Determination of essential functions that need to be continued, uninterrupted, or resumed as soon as possible but not later than 12 hours for up to a minimum of 30 days following a change in normal operations; and

d. Plans and procedures to ensure access to critical communications and information systems necessary to support sustainment of essential functions.

3. Conduct a BPA to identify and document all elements necessary to perform essential functions. The BPA must:

a. Identify and map the functional processes, workflows, activities, resources, personnel expertise, supplies, equipment, infrastructure, systems, data, and alternate locations inherent to the execution of each essential function; and,

b. Be validated and approved by the department or agency head (or designee).

ANNEX C: ORDERS OF SUCCESSION

Succession establishes the formal, sequential assumption of a position's authorities and responsibilities, to the extent not otherwise limited by the law, by the holder of another specified position identified in executive order or other presidential directive or in statute, or by relevant D/A policy or regulation if there is no applicable executive order or 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 the pertinent position.

Orders of succession are formal and sequential listings of positions (rather than specific names of individuals) that identify who is authorized to assume a particular leadership or management role under specific circumstances. By including geographically dispersed leaders at regional, field, or satellite offices in orders of succession, organizations may leverage the advantages of geographical dispersion to ensure roles and responsibilities are effectively transferred during catastrophic emergencies.

In some cases, organizations may have the latitude to develop orders of succession as they deem appropriate, while in other cases succession is prescribed by statute, order, or directive.

In particular, it is critical that organizations comply with the Vacancies Reform Act of 1998, as amended (VRA) (5 U.S.C. §§ 3345-3349d). The VRA prescribes conditions regarding the filling of Federal vacancies to authorize the President, if an appointed officer of an executive agency (defined to include the Executive Office of the President and exclude the U.S. Government Accountability Office) "dies, resigns, or is otherwise unable to perform office functions, to direct a person who serves in an office for which appointment is required to perform such functions temporarily in an acting capacity, subject to specified time limitations." Although the focus of the VRA is to limit the duration of acting officials in senior positions of the Executive Branch, it also influences orders of succession. As such, the VRA frequently comes into play in continuity events.

Orders of succession should be reviewed by the organization's General Counsel or equivalent to ensure legal sufficiency. The General Counsel can also address legal issues related to rules and procedures delegated officials must follow regarding succession; conditions under which succession should occur; the method of notification; and any circumstantial, geographic, or organizational limits. Organizations and subcomponents must establish and document, in writing, orders of succession in advance of a continuity event and, in accordance with applicable laws, to ensure there is an orderly and predefined transition of leadership during any change in normal operations. Orders of succession include but are not limited to administrators, directors, regional or field directors, and key managers. Organizations must revise orders of succession as necessary and distribute the revisions promptly to all organization leadership and Continuity Coordinators and Managers.

Organizations must include orders of succession in their essential records and ensure they are available at all alternate locations.

REQUIREMENTS AND CRITERIA FOR ORDERS OF SUCCESSION:

1. Organizations must establish an order of succession to ensure a designated official is available to serve as acting Organization Head until an official is appointed by the

President or other appropriate authority, replaced by the permanently appointed official, or otherwise relieved of the duty of serving as the acting Organization Head.

2. These orders of succession must comply with the Vacancies Reform Act of 1998, as amended (5 U.S.C. §§ 3345-3349d).
3. Within each order of succession, organizations must include a minimum of three positions (rather than names) permitted to succeed to the identified leadership position.
4. Orders of succession must outline a process and criteria to activate procedures for transition of successors.
5. Procedures must be established for notifying appropriate personnel when succession is implemented.
6. Heads of Category I and II HQ organizations, as identified in PPD-40, must include at least one individual in their orders of succession who is geographically dispersed from the Organization Head and other individuals within the order of succession. Orders of succession must include an individual who is geographically dispersed in all category HQ and non-HQ orders of succession, where feasible.
7. The development and revision of orders of succession must be coordinated with General Counsel to ensure legal sufficiency.

ANNEX D: DELEGATIONS OF AUTHORITY

Delegations of authority ensure the orderly and predetermined transition of responsibilities within an organization during a continuity activation and are closely tied to succession. A written delegation of authority provides successors with the legal authorization to act on behalf of the Organization Head or other officials for specified purposes and to carry out specific duties. Delegations of authority will generally specify a particular function that an individual is authorized to perform and includes restrictions and limitations associated with the authority. Delegations of authority are an essential part of an organization's continuity program and should have sufficient breadth to ensure the organization can perform its essential functions and continuity operations.

Organizations should identify the individuals to whom authorities are delegated by position title and not by name. Delegations of authority are frequently tied to specific positions, but since many delegations require specific training, qualifications, and certification, organizations must also associate some delegations of authority with specific individuals (e.g., delegations for committing funds, contracting, technical direction, and classification authority). Delegations of authority outline conditions under which delegated authority takes effect and the termination process for when authorities are reestablished. Organizations must include written delegations of authority as an essential record and ensure they are available at all alternate locations.

REQUIREMENTS AND CRITERIA FOR DELEGATIONS OF AUTHORITY:

1. In accordance with applicable laws, organizations and subcomponents shall establish and document, in writing, the legal authority for the position of the Organization Head and other key positions. This document should provide detail for officials to make key decisions during a continuity event to include:
    a. Outlining explicitly the authority, including any exceptions to that authority, of an official so designated to exercise organizational direction;
    b. Delineating the limits of authority and accountability;
    c. Outlining the authority of officials to re-delegate functions and activities, as appropriate;
    d. Defining the circumstances under which delegation of authorities would take effect and would be terminated; and,
    e. Incorporating the conditions under which delegations would take place; the method of notification; the duration the delegations may last; conditions when the delegations may be terminated; and, any temporal, geographical, or organizational limitations to the authorities granted by the orders of succession or delegations of authorities, including the ability to re-delegate authorities.
2. Inform those officials listed within the delegations of authority in writing who might be expected to assume authorities in a continuity activation.
3. Establish procedures for notifying appropriate personnel upon implementation of the delegation of authority.

4. The development and revision of delegations of authority must be coordinated with General Counsel to ensure legal sufficiency.

ANNEX E: COMMUNICATIONS AND INFORMATION SYSTEMS

The success of continuity programs is dependent on the availability of and access to communications and information systems with sufficient resilience and contingencies necessary to perform essential functions at primary and alternate locations. These systems must support connectivity among key government leadership, internal elements, other organizations, and the public under all conditions and must be interoperable with essential functions partners and may include the communication of sensitive and/or classified information.

An important area of planning for this capability includes those programs, generally led by Chief Information Officers, that ensure compliance with Federal Information Security Management Act (FISMA) information security requirements and leverage publications including the U.S. Department of Commerce National Institute of Standards and Technology (NIST) Special Publications 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems* and 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* to inform the standards and measures for system evaluations. This contingency planning is often unique to each system, providing preventive measures, recovery strategies, and technical considerations appropriate to the system's information confidentiality, integrity, and availability requirements and the system impact level. Per FISMA, organizations must provide information security for the information and information systems that support the organization's operations and assets including those provided or managed by another organization, contractor, or other source. These programs and processes directly support the resilience of an organization's essential functions.

Organization Continuity Managers should ensure that essential function continuity planning is integrated into and informs communications and information systems contingency and resilience planning efforts. Risk acceptance levels and/or mitigation strategies must be reconciled with user requirements and integrated into the overall plan for the continuance of the essential function(s) the system enables. In addition, Continuity Managers are responsible for ensuring that the requirements of Office of Science and Technology Policy (OSTP) Directives relating to minimum requirements for national leadership communications are integrated with organizational programs to ensure that the national leadership is able to interoperate and communicate with those performing essential functions as appropriate.

REQUIREMENTS AND CRITERIA FOR COMMUNICATIONS AND INFORMATION SYSTEMS:

The following are requirements for the performance of essential functions complement those of OSTP Directives pertaining to executive branch senior leadership and continuity personnel:

1. Provide relevant organization sites and designated continuity personnel with dedicated access to the required minimum communications capabilities in accordance with OSTP directives, to include:
    a. Ensuring communications capabilities are adequately maintained and that continuity personnel are properly trained in their use;

   b. Possessing communications capabilities that support the organization's senior leadership while they are in transit to alternate locations; and,

   c. Planning accordingly for essential functions that require uninterrupted communications and information technology support.

2. Organizations sharing an alternate location and communications capabilities with other organizations have a signed agreement with the system owner to ensure each has adequate access to communications resources.

3. Ensure risk assessments are conducted on all primary and alternate communications and information systems involved in the performance of essential functions, including associated supply chains and facilities such as data processing centers using all-source intelligence and other applicable data and coordinated with Business Impact Analyses (BIAs) for each MEF.

4. Coordinate and integrate Communications and information system-specific planning efforts such as disaster recovery plans and Information System Contingency Plans (ISCPs) with appropriate organizational entities.

   a. System service levels, including maximum allowable downtime and data back-up frequency requirements are coordinated and agreed upon with system owners and reflected in the organization's continuity planning products such as the Continuity Plan and MEF BPA, disaster recovery plans, and service level agreements

5. Activate Wireless Priority Service (WPS) on cellular phones issued to all personnel who perform MEFs and/or other continuity team personnel.

6. Government Emergency Telecommunications Service (GETS) cards:

   a. Pre-position at least one GETS card for emergency use at all primary and continuity facility locations; and,

   b. Issue GETS cards to all continuity team personnel.

7. Ensure primary and alternate locations involved in the performance of MEFs and/or other sites designated by the D/A are enrolled in the Telecommunications Service Priority Restoration Program.

8. Annually review organizational and national continuity communications plans (as appropriate) for accuracy to ensure they are fully capable of supporting essential functions and document the date of review and the names of personnel conducting the review.

ANNEX F: ESSENTIAL RECORDS MANAGEMENT

Essential records, are those records an organization needs to meet operational responsibilities under national security emergencies or other emergency conditions (emergency operating records) or to protect the legal and financial rights of the government and those affected by government activities (legal and financial rights records). Essential records were previously referred to as vital records.

In addition to originals or copies of essential records – regardless of their format – organizations must also consider the protection and use of complementary information systems, technology, applications, infrastructure and references, needed to support the continued performance of essential functions and continuity operations during an activation. The identification, protection, and availability of electronic and hardcopy essential records and electronic information systems needed to support essential functions during all-hazards emergencies are critical elements of a successful continuity plan and program.

Organizations must also protect information that is needed for the resumption of normal operations for reconstitution. Each organization has different functional responsibilities and business needs. An organization decides which records are essential to its operations and then assigns responsibility for maintaining current copies of those records to the appropriate personnel. Organizations should have multiple copies of their essential records in several locations stored on redundant media and in virtual storage environments.

Categories of essential records include the following:

1. Emergency Operating Records: Records and electronic information systems essential to the continued functioning or the reconstitution of an organization during and after a continuity activation. Examples of these types of records are emergency plans and directives, orders of succession, delegations of authority, staffing assignments, and related policy or procedural records. These records provide an organization's continuity personnel with the guidance they need to continue and resume normal operations.
2. Legal and Financial Rights Records: Records that are critical to carrying out an organization's essential legal and financial functions vital to the protection of the legal and financial rights of individuals who are directly affected by that organization's activities. These records include those with such value that their loss would significantly impair the execution of essential functions to the detriment of the legal or financial rights and entitlements of the organization and the affected individual(s). Examples of these records are: accounts receivable files; contracting and acquisition files; official personnel records; Social Security, payroll, retirement, and insurance records; and property management and inventory records. Legal and financial rights records considered critical for continued performance of essential functions and continuity operations should be included in emergency operating records and accessible at the appropriate continuity facility.

National Archives and Records Administration (NARA) provides information on essential (or vital) records regulations and recommended practices for the development and implementation of federal records disaster mitigation and records recovery programs. Federal agencies may find NARA's self-evaluation guide, available at https://www.archives.gov/records-mgmt/vital-

records/appendix-e.html, useful in evaluating their records management procedures for essential records.

REQUIREMENTS AND CRITERIA FOR ESSENTIAL RECORDS MANAGEMENT:

1. An official essential records program must:
    a. Identify and protect those records that specify how an organization will operate in an emergency or disaster including appropriate policies, authorities, and procedures,
    b. Identify and protect those records needed to protect the legal and financial rights of the government and citizens;
    c. Identify and protect those records necessary to the organization's continuity operations including performance of essential functions and reconstitution of normal operations; and,
    d. Include the written designation of an Essential Records Manager and the assignment of responsibilities to specifically designated staff.
2. Ensure continuity personnel have appropriate access at alternate locations to required media (e.g., paper, photographic film, microform, and/or electronic forms), equipment, and instructions for retrieval of essential records including, but not limited to, records stored in cloud-based applications and accessed via the Internet or a Virtual Private Network.
3. Conduct an essential records risk assessment at least annually in order to:
    a. Identify the risks associated with retaining essential records in their current locations and determine the difficulty of reconstituting the records if destroyed;
    b. Identify off-site storage locations and requirements;
    c. Ensure all appropriate storage methods and formats are used; and,
    d. Determine requirements to provide alternate storage locations for duplicate records to guarantee the ready availability of essential records under all conditions and address the capture and protection of work-in-progress essential information.
4. Based on risk assessment results, organizations must implement needed protections for essential records to include dispersing those records to other organization locations or storing those records off-site or electronically in an automated system. When determining and selecting protection methods, it is important to take into account the special equipment, hardware, software, and access rights or permissions needed for each type of storage system or media.
5. Develop and maintain an essential records plan and include a copy of the plan at the alternate sites. An essential records packet is an electronic or hardcopy compilation of key information, instructions, and supporting documentation needed to access essential records in an emergency situation. Packets should be updated or cycled on the same schedule as all other essential information so that they remain current.
6. An essential records packet must include:

a. An electronic and/or hardcopy list of continuity personnel with up-to-date telephone numbers;

b. An inventory of essential records with the precise locations of essential records;

c. Necessary access mechanisms (e.g., keys, access readers);

d. Alternate location information;

e. Access requirements and lists of sources of equipment necessary to access the records (e.g., hardware and software, microform/microfilm readers, internet access, dedicated telephone lines);

f. Lists of records recovery experts and vendors.

g. A copy of the organization's continuity plans.

7. Annually review the organization's essential records program to address new security issues, identify problem areas, and update information to ensure the latest versions are available. This review should also identify any missing essential records.

   a. Incorporate into the program additional essential records generated by program, function, or organizational change to existing programs or functions;

   b. Remove records from the essential records inventory and storage locations when superseded or are no longer applicable according to the records retention schedule or the NARA issued General Records Schedule (GSR 4.1); and,

   c. Document the date of the review and the names of personnel conducting the review.

ANNEX G: ALTERNATE LOCATIONS

Alternate locations refer to alternate sites where essential functions are continued or resumed, and where organizational command and control of essential functions occurs during a catastrophic emergency. An alternate location is a facility sufficiently distanced from the primary facility, within the same region, that is used to conduct continuity operations and is staffed by deployed ERG members. A devolution location is a facility outside the region of the primary facility that is used to conduct continuity operations and is staffed by the DERG. All category I and II HQ organizations, and organization components that perform MEFs and PMEFs must have a physical alternate site(s) and a physical devolution site(s) that support continuity and devolution operations. Telework may be used to augment continuity, but due to its voluntary nature and potential risks of communications outages, should not be relied upon as an organization's primary continuity option.

Organizations should consider locations that are not uniquely susceptible to risks associated with natural disasters and select facilities in locations that provide the continuity facilities with power, telecommunication services, and Internet access separate from those grids that provide their services to the primary facility, whenever possible. Organizations should work to identify alternate locations that would not be affected by the same catastrophic event or emergency which is driving operations away from the primary location. Selection should be based upon the general principle of proximity away from the organization's primary location of operation. Alternate usage of existing facilities and telework options enhance the organization's resilience and continuity capacity.

Organizations should consider maintaining multiple sites that could be used based upon varying degrees of risk and severity of threat. For example, an organization may select an alternate site in the immediate geographic location as its primary location of operation for use in the event of a burst pipe or fire occurring in the main building. Organizations must also maintain alternate sites located further away for use in situations causing a higher degree of damage and reducing the ability to operate locally (e.g., flood, earthquake). Ultimately, the Organization Head is responsible for deciding which alternate locations will be used to ensure continued execution of the organization's MEFs and PMEFs.

There is a direct relationship between an organization's COOP plan and telework. The two programs share the basic objective of performing and maintaining an organization's functions from an alternative location. Telework can assist the sustainment of essential functions during a change to the normal operating status such as a pandemic or a flood that causes a partial building closure. However, telework may not be a viable strategy for continuing essential functions during all events (e.g., cyber events, mass power outage). If an organization plans to utilize telework to continue essential functions, this must be documented in its continuity plan. Organizations should work with their human resources offices and Telework Managing Officer while leveraging continuity personnel to support continuity operations in a telework environment.

When using telework as a strategy to support essential functions during a continuity event, organizations must identify which functions can be conducted via telework, including evaluating the use of telework for supporting extended continuity operations and use by non-ERG personnel. Organizations must adhere to OPM and internal policy and guidance governing the use of telework, provide protection of information and information systems during telework

activities according to government standards, and provide access to essential records, databases, and the robust communications necessary to sustain an organization's essential functions at telework locations. Organizations should coordinate with their Chief Information Officer to identify equipment and technical support requirements for personnel identified as telework-capable.

All Category I and II HQ organizations and components that perform MEFs that directly support PMEFs must continue essential functions from an alternate location; telework is not to be used as a primary alternate facility but as a tool to accommodate an organization's continuity strategy for those essential functions and supporting tasks authorized for telework. When identifying and preparing continuity facilities for operation, organizations should maximize the use of existing infrastructure, and should leverage technology to enhance the effectiveness of continuity programs through the use of telework, mobile work, and joint or shared facilities.

1. Continuity facilities are classified in the following three ways:
    a. **Hot site:** Hot sites are locations that operate 24 hours a day with fully operational equipment and capacity to immediately assume operations upon loss of the primary facility. A hot continuity facility requires on-site telecommunications, information, infrastructure, equipment, back-up data repositories, and personnel required to sustain essential functions.
    b. **Warm site:** Locations that have a minimum acceptable level of infrastructure in-place, and also possess the IT and telecommunications equipment to become operational as soon as possible, but not later than 12 hours after continuity activation. In order to become active, a warm facility requires additional personnel, equipment, supplies, software, or customization. Warm sites generally possess the resources necessary to sustain critical mission/business processes, but lack the capacity to activate all systems or components.
    c. **Cold site:** Facilities that are neither staffed nor operational on a daily basis. Telecommunications, IT equipment, and other infrastructure is typically present at the location, however teams of specialized personnel must be deployed to activate the systems before the site can become operational. Basic infrastructure and environmental controls are present (e.g., electrical and heating, ventilation and air conditioning systems), yet systems are not continuously active.
2. Organizations may make use of existing space for alternate locations including:
    a. Remote/offsite training facilities: These sites include training centers located near an organization's primary facility, but with sufficient distance to afford geographical dispersion.
    b. Regional or field offices: Regional or field offices may serve as suitable alternate locations for HQ operations.
    c. Remote HQ operations: HQ operations that occupy geographically dispersed offices may designate one or more of these locations as an alternate location.
    d. Co-location: An organization may relocate to another organization's facilities. The relocating organization might occupy available space in the receiving organization's HQ, training facilities, or field offices. Co-location is often coordinated via

reciprocal agreements in which each organization agrees to host the other in a contingency that may affect only one of the organizations.

e. Space procured and maintained by the U.S. General Services Administration (GSA): An organization may enlist the assistance of GSA to acquire, equip, and sustain privately and/or federally owned and leased space to accommodate continuity requirements.

f. Space procured and maintained by another organization: Some organizations other than GSA offer space procurement services for use by organizations who require an alternate location.

g. Joint-use continuity facilities: Several organizations may pool resources to acquire a joint continuity facility to be used as their alternate location. Organizations use care to avoid over-commitment of joint-use facilities during continuity activations. Additionally it is imperative that each organization have designated resources in joint-use facilities.

h. Alternate use of existing facilities: In certain types of continuity activations, organizations may use a combination of existing facilities and strategies, such as social distancing, to support continuity operations.

In order to assist in the scoping of U.S. Federal Government continuity plans and programs, PPD-40 requires Federal D/As to internally identify and document the locations of continuity facilities via the completion and submission of GSA Standard Form (SF) 336, GSA Alternate Facility Reporting Form.

a. D/As with access to classified systems must register and annually submit their completed forms via https://gsapergamum.gold.ic.gov.

b. D/As may access this form via the internet at http://www.gsa.gov/forms, and may submit their unclassified information annually via fax to 817-207-6314 or 312-353-9307.

c. Organizations are required to review and re-submit their SF-336 to GSA annually.

d. Organizations must submit preliminary site documentation by using the SF-336 to gain approval before committing resources. The SF-336 shall be submitted at least 30 days prior to the formal commitment or contract to occupy the facility.

e. In the event an organization no longer requires a facility currently in use, they must notify GSA 30 days prior to vacating the site by submitting an updated SF-336.

Organizations may contact GSA's Office of Mission Assurance at 202-219-0338 for further instructions.

REQUIREMENTS AND CRITERIA FOR ALTERNATE LOCATIONS:

1. Organizations must perform the following actions (at a minimum) to support deployment of ERGs and DERGs:
    a. Establish and maintain alternation locations for relocation during disruptions to normal operations.
    b. Review alternate locations for suitability and functionality at least annually, validate continuity requirements, and document the date and names of personnel conducting the review/validation.

c. Establish and implement procedures for the orientation, processing, and reception of continuity personnel.

d. Coordinate with site facility managers to ensure availability of space and services.

2. Alternate locations that are neither owned nor leased, must have a current, signed MOA/MOU with the owner or occupant of the facility, and must review the MOA/MOU annually, or following leadership changes. At a minimum, MOAs/MOUs must specify:

   a. The maximum time required for notification of the owner/occupant to have the facility configured for occupancy.

   b. Details of the space and services to be provided at the facility.

   c. Access control procedures to the allocated space during occupancy.

   d. The dates and names of personnel conducting the review.

3. Organizations must ensure the following capabilities exist at alternate locations prior to activation, or become available as soon as possible but not later than 12 hours after activation:

   a. The capability to ensure performance of essential functions with minimal disruption of operations, for a minimum of 30 days or until normal operations are resumed.

   b. Replication of essential capabilities by providing systems and configurations that are used in daily activities.

   c. Capability to access and use essential records necessary to conduct continuity operations.

   d. Interoperable communications, including secure communications if appropriate, with all identified internal and external stakeholders.

   e. Computer equipment, software, information systems, and other automated data processing equipment necessary to conduct continuity operations. Information technology systems must be current.

   f. The availability of essential resources such as food, water, fuel, medical and municipal services to ensure the health, safety, and security of the facility and personnel.

   g. Emergency/back-up power capability in the event the primary power source is disrupted.

   h. Lodging to support deployed continuity personnel at or near the facility. Options include billeting within the facility, private or commercial facilities (e.g., hotels, motels) and/or use of employee residences if within commuting distance.

   i. A transportation support plan that details transportation to, from, and at the physical alternate location for ERG members.

   j. Sufficient levels of physical and information security to protect against all threats, as identified in the facility's risk assessment and physical security surveys. This

includes sufficient personnel to provide perimeter, access, and internal security, as required by organizational policy.

4. Organizations must assess each activity, task, or responsibility associated with continuity operations to determine if it is capable of being performed via telework or whether it must be performed, in part or in whole, at an alternate location. This includes:
    a. Supporting functions or capabilities necessary to ensure the continued performance of essential functions;
    b. Ensuring continuance of a viable continuity capability in the event that telework is not a viable option (e.g., significant power and/or telecommunications infrastructure degradation); and,
    c. Identifying employees who are unable to perform designated functions through telework and are therefore required to be onsite to perform continuity operations; the organization must classify the associated risk exposure level of the position/job to an infectious biological incident. Organizations must notify these employees in advance of a continuity event that they are expected to work onsite during an infectious biological incident and provide appropriate or necessary administrative controls, training, and/or personal protective equipment.
5. Organizations must establish and maintain plans, policies, and procedures for telework as part of the organization's continuity strategy. This includes:
    a. Coordinating with the organization's designated Telework Managing Officer when developing and integrating telework considerations into the organization's continuity plan; and,
    b. Notifying continuity personnel that they are filling positions identified as telework-capable.
6. Organizations must comply with GSA's requirement for completion and submission of the SF-336, GSA Alternate Facility Reporting Form.
    a. Initial submission of SF-336 to GSA.
    b. Annual review and or/resubmission of SF-336 to GSA.

ANNEX H: HUMAN RESOURCES

An organization's personnel are its most valuable resource. Choosing the right personnel to staff an organization's continuity team is critical. Continuity team personnel include executive and senior leadership, staff with the technical expertise, and those that perform, conduct, or support continuity operations and essential functions. The ERG is comprised of primary and alternate staff who relocate during a continuity event, while the DERG is comprised of alternate individuals geographically dispersed from the primary site. Both groups perform, or ensure the performance of, the organization's essential functions and other continuity operations.

Organizations are also responsible for utilizing and supporting non-continuity personnel who may be affected by a continuity activation. Organizations should address expectations for non-continuity personnel in continuity plans and/or procedures as well as in emergency plans such as an Occupant Emergency Plan (OEP). Personnel accountability is a critical capability for all organizations. Organizations must have the means and process in place to contact and account for employees and they must communicate this process to all employees.

Each Organization Head, or designee, has the authority and responsibility to identify and designate those personnel that he/she determines to be critical to the organization's operations in any change in normal operating status, such as a continuity activation, OEP activation, or closure procedures that prevents employees from reporting to their normal operating facility.

Organizations must facilitate dialogue among their respective head of Human Resources, Telework Managing Officer, and Continuity Manager when developing continuity plans and programs. Such topics that should be addressed include the designation of employees who are deemed critical and who must report to the continuity facility, the designation of employees who are telework-capable to support continuity operations, and those employees that will be excused from duty due to the emergency situation (i.e., those that have not been designated as critical employees).

REQUIREMENTS AND CRITERIA FOR HUMAN RESOURCES:

1. Develop and implement processes to identify, document, and prepare continuity personnel to conduct or support continuity operations.
    a. Clearly define the expectations, roles, and responsibilities of continuity personnel.
    b. Inform continuity personnel and alternates in writing of their continuity roles and responsibilities. Organizations must also obtain a signed acceptance of these roles and responsibilities. See the sample memorandum on page H-4, "*Appointment as an Emergency Relocation Group (ERG) Member*."
    c. Maintain a roster of trained personnel capable of performing continuity operations. The roster should include not only primary personnel but also alternates or back-up personnel in sufficient quantity. Rosters must be updated periodically and include, at a minimum, names and office and government-issued cell telephone numbers.
    d. If bargaining unit employees are included as continuity personnel, organizations must ensure that all applicable collective bargaining obligations are satisfied.

2. Provide guidance to continuity personnel on individual preparedness measures they should take to ensure response to a continuity activation.
    a. Recommend the content and maintenance of drive-away kits for deploying continuity personnel.
    b. Provide guidance to all staff in preparing, planning, and staying informed during an emergency, including procuring an emergency supply kit, making a family emergency plan, and being informed about the different types of emergencies that could occur and their appropriate responses.
3. Develop a strategy and plan for utilizing and supporting non-continuity personnel during continuity activations.
    a. Organizations must provide the ability to communicate with and coordinate activities with non-continuity personnel.
    b. Provide guidance on roles and responsibilities of non-continuity personnel.

       Organizations must communicate how, and the extent to which, non-continuity personnel are expected to remain in contact with their organizations.
4. Work with the Human Resources Office to develop and promulgate processes or procedures on how the organization will account for personnel in the affected area during a continuity event.
    a. Continuity team personnel must be accounted for no later than 12 hours after activation.
    b. All employees within the affected area must be accounted for within five days after activation of an organization's continuity plan.
5. Implement a process to communicate the organization's operating status to all staff and stakeholders (e.g., 1-800-hotline, website, radio or TV broadcast, email).
    a. Implement a process to contact all staff, including contractors, in the event of an emergency in the affected area.
    b. Establish procedures and provide the ability to communicate and coordinate activities with all personnel, continuity facilities and support teams, entities the affected organization interacts with (other organizations, customers, and stakeholders) before, during, and after a continuity event, including alerts and notification.
    c. Communicate how, and the extent to which, employees are expected to remain in contact with their organizations during any emergency situation.
6. Develop and implement a process to communicate guidance on pay, leave, staffing, and other human resources flexibilities to all staff.

a. Provide information or reference provisions and procedures to assist disaster survivors regarding special human resources concerns following a continuity event.

b. Establish and maintain procedures to provide guidance to non-continuity personnel.

c. Coordinate in advance with labor unions in developing and bargaining over such procedures where bargaining unit employees are impacted.

SAMPLE MEMORANDUM

MEMORANDUM FOR: (NAME OF ERG MEMBER)

FROM: (SUPERVISOR NAME, OFFICE)

SUBJECT: Appointment as an Emergency Relocation Group Member

You have been identified as critical to agency operations in an emergency situation. You are hereby appointed as an Emergency Relocation Group (ERG) member for (OFFICE NAME). ERG members are select personnel assigned to perform essential functions when such functions can no longer be supported from the (PRIMARY/OTHER) facility due to a local, regional, or national change in operating status and the need to operate from an alternate operating facility exists. ERG members deploy to their alternate location(s) to establish an operational capability and to perform essential functions within 12 hours of a continuity of operations activation. In a continuity activation, you shall deploy to (ALTERNATE LOCATION). Deployment to the alternate location may last for up to 30 days after an event or until normal operations can be resumed.

Each ERG member is selected by his/her respective department head based upon:

- The identification of predetermined essential functions that must be performed, regardless of the operational status of the (PRIMARY/OTHER) building.
- The employee's knowledge and expertise in performing these essential functions.
- The employee's ability to rapidly deploy to the alternate location in an emergency situation.
- The employee's ability to be precluded from other emergency assignments.

I understand and accept my assignment as an ERG member for (OFFICE NAME) as outlined above.

_____ _____

Signature of ERG member *Date*

ANNEX I: DEVOLUTION

Devolution is the capability to transfer statutory authority and responsibility from an organization's primary operating staff and facilities to other designated staff and alternate locations to sustain essential functions. A continuity plan's devolution option addresses how an organization will identify and transfer organizational command and control, as well as responsibility for performing essential functions to personnel at a geographically dispersed location unaffected by the incident.

Organizations may activate their DERG as a short-term option while ERG members relocate to their alternate location(s). Additionally, organizations may choose to partially devolve by transferring responsibilities for select essential functions or devolve to multiple sites by transferring responsibilities for particular essential functions to various sites.

The devolution counterpart must have the capability to perform essential functions as soon as possible but not later than 12 hours after devolution plan activation and must be able to sustain operations for a minimum of 30 days or until normal operations are resumed. When selecting a devolution location, organizations must consider the capabilities of the location to ensure it has the communications, systems, equipment, and resources pre-positioned or available within the accepted timeframe to assume responsibility for performance of essential functions. Personnel assigned devolution responsibilities who perform continuity operations are referred to as the DERG. The organization must prepare the DERG to conduct continuity operations through its test, training, and exercise program. Organizations should also consider the development of support documentation such as training and job aids, standard operating procedures, desk guides, and handbooks.

REQUIREMENTS AND CRITERIA FOR DEVOLUTION:

1. Develop a plan for a devolution option for continuity to address conduct of essential functions when the primary operating facility, and/or ERG members are not available.
    a. The plan must identify both active and passive triggers that result in the activation and implementation of the devolution plan.
    b. The plan must specify how and when direction and control of organization operations will transfer to and from the devolution location.
    c. Organizations must determine the necessary resources to facilitate an immediate and seamless transfer of functions to the devolution location.
    d. The plan must list the necessary resources, such as equipment and materials, to facilitate the performance of essential functions at the devolution site.
    e. The plan must address the following elements of continuity: program management, plans, and procedures; essential functions; orders of succession; delegations of authority; continuity communications and information systems; essential records management; alternate locations; telework; human resources; devolution; reconstitution; and test, training and exercise.
    f. The plan must outline procedures for the transition of responsibilities to personnel at the primary operating facilities upon termination of devolution.

2. Maintain a roster of trained personnel capable of performing devolution operations (DERG). The roster should include not only primary personnel but also alternates or back-up personnel in sufficient quantity. Rosters must be updated periodically and include, at a minimum, names and office and government-issued cell telephone numbers.
3. Provide annual training on roles and responsibilities for personnel, including host or contractor personnel, who are assigned to activate, support, and sustain devolution operations. Training must include:
    a. Organization devolution plan processes and procedures;
    b. Communications and IT systems that will be used during devolution operations;
    c. Identification, protection, and availability of electronic and hardcopy documents, references, records, information systems, and data management software and equipment (including classified and other sensitive data) needed to support devolved essential functions during devolution operations; and,
    d. How the organization identifies and conducts its essential functions during an increased threat situation or in the aftermath of a catastrophic emergency that activates the devolution plan.
4. Conduct a biennial exercise for DERG members to demonstrate their familiarity with devolution procedures. This exercise may be part of annual continuity exercises (Eagle Horizon) or it may be conducted separately.
    a. Familiarize DERG members with devolution plan processes and procedures.
    b. Demonstrate familiarity with reconstitution plans and procedures for the original primary operating facility and replacement primary operating facility.

ANNEX J: RECONSTITUTION

PPD-40 defines reconstitution as "the process by which surviving and/or replacement D/A personnel resume normal operations." Reconstitution embodies the ability of an organization to recover from a continuity activation that disrupts normal operations so that the organization can resume its operations as a fully functional entity of the Federal Government.

As an element of continuity, reconstitution simultaneously sustains essential functions while coordinating the resumption of normal operations. Since reconstitution planning begins at the start of a continuity event, organizations should identify a reconstitution team with leadership, staff, and resources dedicated and separate from existing continuity support.

In some cases, extensive coordination may be necessary to procure a new operating facility, backfill staff, reestablish communications and IT infrastructure, restore essential records, and take other actions to return the organization to normal operations. Some of the activities involved with reconstitution include:

1. Assessing the status of the affected facility or facilities, personnel, systems, records, and other resources.
2. Determining how much time is needed to replace, repair, or otherwise reconstitute facilities, personnel, systems, records, and other resources.
3. Supervising facility repairs or other reconstitution efforts, if appropriate.
4. Notifying decision makers of the status of reconstitution efforts, including estimates of when the repairs will be completed, if appropriate.
5. Implementing a priority-based phased approach to reconstitution.
6. Periodically providing status updates of reconstitution activities through the submission of Reconstitution Status Reports (RSRs) to FEMA through the RRS.

Identifying reconstitution requirements assist organizations to identify, develop, and coordinate a plan to resume normal operations. Just as an organization's capacity to perform essential functions relies upon the four pillars of continuity – leadership, staff, communications, and facilities – an organization's capability to reconstitute likewise depends upon these pillars. Communications enables an organization to notify staff that the necessity for continuity operations no longer exists and to provide instructions for resumption of normal operations. Non-ERG staff augment the ERG to resume non-essential functions. Leadership determines priorities and supervises the orderly return to normal operation. Organizations assess the status of affected facilities and transition back into the primary operating facility or another designated facility. As detailed in PPD-40, DHS/FEMA will facilitate and coordinate the activities of GSA, Office of Personnel Management (OPM), and NARA in the implementation of reconstitution of the Executive Office of the President and D/As and will inform the NCC of the Executive Branch's reconstitution status.

FEMA, GSA, OPM, and NARA support reconstitution of the Executive Branch in the following areas:

- **FEMA:** Monitors and reports the continuity status of Executive Branch organizations, assesses potential impact to COOP, facilitates information sharing among operational nodes of the Federal Government, provides continuity input to the DHS Common

Operating Picture, monitors the operation of continuity communications systems, and assists with reconstitution of the Executive Branch.

- **GSA:** Provides facility services for temporary space acquisition or identification of a new permanent facility to include contracted support as well as coordinating repairs to damaged facilities.
- **OPM:** Provides assistance on human resources policy to ensure the Federal Government has the necessary tools to support a civilian workforce.
- **NARA:** Provides guidance and advice to reconstitution teams regarding preservation of records; logistics, stabilizing, securing, and managing archives; and assistance with records and recovery service contracts.

PPD-40 requires Federal D/As to report reconstitution requirements to GSA. To assist in scoping of the Federal Government's reconstitution plans and programs, organizations should internally identify and document anticipated reconstitution needs for their HQ facilities located within the NCR by completing and submitting Standard Form 2050 (SF-2050), Reconstitution Questionnaire.

a. D/As with access to classified systems must annually register and submit their completed forms to https://gsapergamum.gold.ic.gov.

b. D/As without access to classified systems can access the form via the internet at http://www.gsa.gov/forms and can annually submit their unclassified information via fax to 817-207-6314 or 312-353-9307.

c. Organizations are required to annually review and submit their SF-2050 to GSA.

Organizations may contact GSA's Office of Mission Assurance at 202-219-0338 for further instructions.

REQUIREMENTS AND CRITERIA FOR RECONSTITUTION OPERATIONS:

1. Designation of a Reconstitution Manager to oversee all phases of the reconstitution process.
2. Develop a plan to recover from the effects of a disruption in operating conditions and to support the transition back to normal operations once a threat or disruption has passed. This plan must:
    a. Determine how the organization will assess the status of its affected personnel, assets, and facilities;
    b. Outline the necessary procedures for conducting a smooth transition from the continuity facility to either the normal primary facility, another temporary facility, or a new permanent facility;
    c. Detail how the organization will verify operational capability and availability of systems, communications, essential records, infrastructure, and other required resources. Establish that the organization is fully capable of accomplishing all essential functions and operations at the new or restored facility;
    d. Identify how the organization will determine if any records were affected by the incident to ensure an effective transition or recovery of essential records;

e. Include redeployment plans for phasing down continuity facility operations and supervising the return of operations, personnel, records, and equipment to the primary or other operating facility in a priority-based approach; and,

f. Detail how the organization will instruct all personnel on how to resume normal operations.

3. Organizations must comply with GSA's requirement for completion and submission of GSA Standard Form 2050 (SF-2050), Reconstitution Questionnaire.

   a. Initial submission of SF-2050 to GSA.

   b. Annual review and/or resubmission of SF-2050 to GSA.

ANNEX K: TEST, TRAINING, AND EXERCISE PROGRAM

An effective test, training, and exercise (TT&E) program is necessary for organizations to prepare and validate continuity plans and programs in order to verify the Executive Branch's ability to perform essential functions during a change in normal operating conditions. The TT&E of continuity capabilities is essential to demonstrating, assessing, and improving an organization's ability to execute its continuity program, plans, and procedures.

In accordance with PPD-40, it is critical for organizations to plan and conduct routine internal TT&E and participate in annual TT&E events in order to evaluate program readiness and ensure adequacy and viability of continuity plans and communications and IT systems.

- **Testing:** Demonstrates the correct operation of all equipment, procedures, processes, and systems that support an organization's continuity infrastructure. This ensures that resources and procedures are kept in a constant state of readiness. Testing an organization's policies, plans, and procedures cultivates better organizational knowledge, identifies gaps in coverage, and validates existing plans and programs.
- **Training:** Familiarizes continuity personnel with their roles and responsibilities to support the performance of an organization's continuity operations. Training results in a better understanding of an organization's continuity program, processes, and procedures.
- **Exercise:** An exercise is an instrument to train for, assess, practice, and improve continuity capabilities in a risk-free environment. Exercises can be used for testing and validating policies, plans, procedures, training, equipment, and interagency agreements; clarifying and training personnel in roles and responsibilities; improving interagency coordination and communications; improving individual performance; identifying gaps in resources; and identifying opportunities for improvement. The Homeland Security Exercise and Evaluation Program (HSEEP) provides guiding principles for exercise programs, as well as a common approach to exercise program management, design, development, conduct, evaluation, and improvement planning.

REQUIREMENTS AND CRITERIA FOR TT&E:

Annual requirements in this annex are defined as occurring during the federal fiscal year. The critical requirements within TT&E must address the following:

Program Management

1. Incorporate continuity requirements into an organization-wide TT&E program. Conduct and document activities that identify the organization's processes and requirements for the training and preparedness of continuity personnel.
    a. Document all conducted TT&E events, including the date of the event, those personnel participating in the event, and the outcomes of the event. During biennial organization assessments, documentation must be made available to FEMA evaluators.
    b. Utilize an all-hazards approach to affirm the viability of continuity plans and programs using threats, hazards, and vulnerabilities identified through organizational risk assessments.

Testing

An organization's testing program must include and document:

1. Alert and notification testing:
    a. Annual testing of alert and notification procedures for continuity personnel.
    b. Quarterly testing of such procedures for personnel at the organization's HQ.
2. Testing for information systems and essential records:
    a. Annual testing of recovery strategies (i.e., disaster recovery plans and/or IT contingency plans) for essential records (both classified and unclassified), critical information systems (both classified and unclassified), services, and data.
    b. Annual testing of the capabilities for protecting essential records and information systems (both classified and unclassified) and for providing access to them from alternate locations.
3. Quarterly testing of the internal and external interoperability and viability of primary and contingency communications and information technology systems.
4. Annual testing of primary and backup infrastructure systems and services, such as power, water, and fuel, at alternate locations.
5. Annual testing of telework capabilities, to include IT infrastructure required to support telework options during a continuity activation.

Training

An organization's training program must include and document:

1. Annual continuity awareness briefings for the entire workforce to include new personnel as they onboard.
2. Annual training on roles and responsibilities for all continuity personnel, including host or contractor personnel, who are assigned to activate, support, and sustain continuity operations. Training must include:
    a. Organization continuity plans that involve using or relocating to alternate locations or other work arrangements, such as telework;
    b. Reconstitution plans and procedures to resume normal operations at a primary operating facility or a replacement primary operating facility;
    c. Communications and IT system planning necessary to support or sustain continuity operations; and,
    d. How to identify, protect, and make available electronic and hardcopy essential records, documents, references, records, information systems, and data management software and equipment (including classified and other sensitive data) needed to support or sustain continuity operations.
3. Annual training for the organization's leadership on its essential functions, succession, continuity communications, and deployment requirements.

4. Annual training for all organization and sub-component personnel designated within the orders of succession for the Organization Head or other key positions who assume the authority and responsibility of the organization's leadership if that leadership is incapacitated or becomes otherwise unavailable during a continuity activation.
5. Annual training for those officials listed within the delegations of authority on all pre-delegated authorities, including limitations, conditions, and restrictions that have been delegated.

Exercises

An organization's exercise program must include and document:

1. An exercise plan that includes a cycle of events that incorporates evaluations, After Action Reports (AARs), and lessons learned into the development and implementation of an Improvement Plan (IP).
2. An annual exercise for continuity personnel to demonstrate their familiarity with continuity plans and procedures and to validate the organization's capability to continue its essential functions. The exercise must:
    a. Include the deliberate and preplanned movement of ERG members to an alternate site;
    b. Test and validate intra- and interagency communications capabilities;
    c. Verify that data and records required to support essential functions at alternate locations are sufficient, complete, current, and accessible to ERG members;
    d. Maintain situational awareness and outreach with internal and external interdependencies identified in the organization's continuity plan with respect to performance of the essential functions of the organization; and,
    e. Demonstrate capability to continue essential functions from telework sites, if used as a continuity strategy, to include accessing and using records, communications, and systems.
3. D/A HQ continuity personnel and those components who support organizational MEFs/PMEFs are mandated to participate in a continuity exercise annually. FEMA NCP-sponsored Eagle Horizon exercises are incorporated in the FEMA/National Exercise Division (NED)-led National Exercise Program. Organizations are externally evaluated during Eagle Horizon for continuity capabilities every two years. Organizations must:
    a. Provide evaluators, data collectors, facilitators, controllers, and other required exercise personnel, as requested;
    b. Develop internal exercise objectives and injects that support essential functions;
    c. Conduct a comprehensive debriefing or hot wash after each exercise, which allows participants to identify systemic weaknesses in plans and procedures and to recommend revisions to the organization's continuity plan; and,
    d. Develop and incorporate identified strengths and areas for improvement in the overall Eagle Horizon AAR/IP.

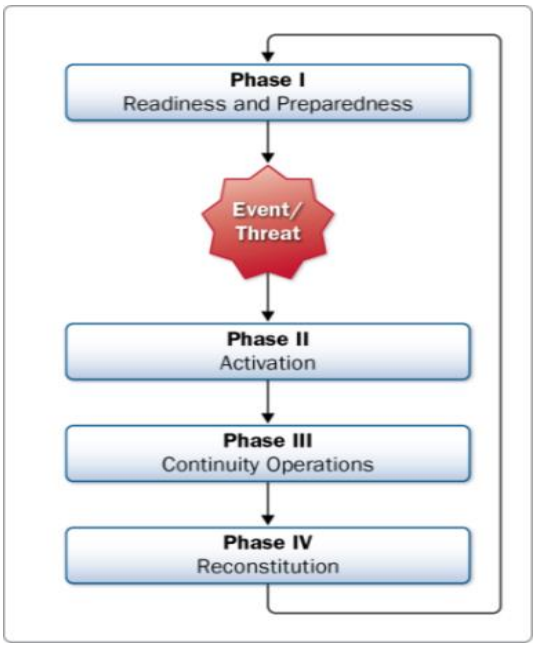
4. Conduct a biennial exercise for ERG members to demonstrate their familiarity with reconstitution procedures for transitioning from a continuity environment to normal operations, when appropriate.

ANNEX L: CONTINUITY OPERATIONAL PHASES AND IMPLEMENTATION

Implementation of a continuity plan is intended to continue or rapidly resume essential functions following a change to normal operating conditions. The continuous performance of essential functions is critical to an organization's resilience during a continuity event.

There are four phases of continuity operations: readiness and preparedness, activation, continuity operations, and reconstitution. These four phases should be used to build continuity processes and procedures, to establish goals and objectives, and to support the performance of organizational MEFs/PMEFs during a catastrophic emergency.

Figure L-1. Four Phases of Continuity



Readiness and Preparedness

Readiness is the ability of an organization to respond to a continuity activation. Although readiness is a function of planning and training, it is ultimately the responsibility of leadership. Leadership must ensure that its organization can perform continuity operations, including the performance of essential functions before, during, and after all-hazards emergencies. This phase includes all continuity readiness and preparedness activities, such as the development, review, and revision of continuity plans, orders of succession, and delegations of authority; TT&E; and risk management.

Non-HQ organizations may consider creating a continuity readiness posture similar to the Executive Branch's COGCON system for HQ organizations, which is presented in Table L-1, COGCON Matrix, on page L-3.

Readiness and preparedness activities include monthly submission of Readiness Reporting System (RRS) reports, which provide FEMA and the NCC with an assessment of an organization's capacity to support continuity operations. Organizational HQs must submit

monthly continuity readiness status information via RRS no later than the monthly deadline set by FEMA NCP. These assessments will be used to determine the organization's continuity readiness posture, and to help identify needs and gaps.

For assistance with the submission of the monthly continuity assessment, contact the FEMA RRS Team by email at rrs-submission@fema.dhs.gov.

Executive Branch Continuity of Government Readiness Conditions (COGCON) Matrix

Readiness Level	Operations	Staffing Level	Time to Transition to Successive Stages	Communications	Succession	Impact on D/As
COGCON 4	• Continue to perform HQ business functions at normal location(s). • Maintain alternate operating facility (ies) in accordance with agency continuity plans to ensure readiness for activation at all times. • Conduct training and exercise activities in accordance with agency continuity and TT&E plan(s) to ensure personnel readiness.	• No staffing required to be at alternate facility (ies). • Maintain normal delegations and devolution of authority to ensure performance of essential functions to respond to a no-notice event.	• Continuity plan is fully operational within 12 hours.	• Test all internal agency communications capabilities between normal operating locations (HQ and other) and alternate operating facility (ies) no less than quarterly. • Test all communications capabilities at all alternate operating facility (ies) with applicable interagency partners no less than quarterly.	• No special measures to protect or track the location of agency leadership and successors. • Ensure delegations of authority to lead D/As are in place for senior personnel located outside of the NCR.	• No additional requirements.
COGCON 3	• Continue to perform HQ business functions at normal location(s). • Maintain alternate operating facility (ies) in accordance with agency continuity plans to ensure readiness for activation at all times. • Conduct additional training activities to increase personnel readiness (e.g., Team tabletops, review recall lists, review plans and procedures).	• No staffing required to be at alternate operating facility (ies) unless necessary to meet 8-hour operational requirement. • Maintain normal delegations and devolution of authority to ensure performance of essential functions to response to a no-notice event.	• Continuity plan is fully operational within 8 hours. • 4 hours to COGCON 2.	• Conduct at least one additional internal agency communications test between normal operating locations (HQ and other) and alternate operating facility (ies) within 24 hours.	• Track the locations of agency leaders and their successors on daily basis.	• Additional staff time for communication testing and tracking agency leadership. • Potential shorter response times for basic staffing of alternate facility (ies).
COGCON 2	• Continue to perform HQ business functions at normal location(s). • Monitor/track major HQ activities. • Maintain alternate operating facility (ies) in accordance with agency continuity plans to ensure readiness for activation at all times. • Take appropriate steps to ensure alternate operating facility (ies) can be activated with 4-hours' notice.	• Deploy sufficient staff to alternate operating facility (ies) to allow activation with 4-hours' notice.	• Continuity plan is fully operational within 4 hours. • 4 hours to COGCON 1.	• Conduct internal agency communications tests between normal operating locations (HQ and other) and alternate operating facility (ies) within 24 hours and repeat not less than weekly. • Conduct communication tests at all alternate operating facility (ies) with applicable interagency partners within 48 hours and repeat not less than weekly.	• Track the locations of agency leaders and their successors on daily basis. • Ensure at least one HQ-level agency successor is out of the NCR at all times.	• Potential increased travel requirements for agency leadership. • Some staff is required to work from alternate location(s). • Potential shorter response times for additional staffing of alternate facility (ies).
COGCON 1	• Continue to perform HQ business functions at normal location(s) as appropriate. • Monitor/track major HQ activities. • Perform day-to-day functions at alternate facility (ies) as appropriate. • Take appropriate steps to ensure alternate operating facility (ies) can be activated with no notice.	• Deploy sufficient staffing to alternate operating facility (ies) to perform essential functions with no notice.	• Agency HQ continuity plan activated immediately and report operational status within 2 hours.	• Test internal agency communications between normal operating locations (HQ and other) and alternate operating facility (ies) daily. • Conduct communication tests at all alternate operating facility (ies) with applicable interagency partners daily.	• Track the locations of agency leaders and their successors on a daily basis. • At least one HQ-level agency successor must be at alternate operating facility (ies).	• Some agency leaders work from alternate facility (ies). • Significant number of staff are required to work from alternate location(s).

Table L-1: COGCON Matrix

Activation Phase (0-12 Hours)

This phase should include the activation of plans, procedures, and schedules for the continuation of essential functions. Continuity personnel must be fully operational at the alternate facility as soon as possible but no later than 12 hours after continuity activation.

The activation and implementation of a continuity plan and its associated procedures may require the use of alternate locations, depending upon the incident and its effect on normal operations. Examples of scenarios that may require activation of continuity plans and procedures include the following:

1. An organization or the region in which the organization is located receives notification of a credible threat that leads the organization to enhance its readiness posture and prepare to take actions as necessary.
2. An organization experiences a disruption in normal operations that requires the relocation of ERG members to an alternate site.
3. An organization's ERG and/or primary operating facility and continuity facility are unavailable or inaccessible, necessitating a shift of operations to a devolution site.
4. Mass evacuation of a large geographic area affected by an incident of threat.

The activation phase includes the following activities:

1. Occurrence of an event or the threat of an event.
2. Reviewing, analyzing, and deciding to activate continuity and/or devolution plans.
3. Alerting and notifying the ERG and/or DERG.
4. Relocating, if necessary, to alternate sites.
5. Devolving, if necessary, to devolution sites.
6. Accounting for ERG and/or DERG members.
7. Identifying available organizational leadership.
8. Submitting the Quick Look/Continuity Status Report (QL/CSR) through RRS no later than two (2) hours after receipt of the COGCON change. The QL/CSR component provides an **immediate**, aggregated view of D/As' responses following directed COGCON change. Reports are submitted via the RRS using the FEMA-provided RSA token at https://rrs.csd.disa.mil/. For assistance with report submission, contact the RRS Team by email at rrs-submission@fema.dhs.gov.

Continuity Operations Phase

This phase includes the following activities to continue essential functions:

1. Accountability of personnel in the affected area during continuity operations.
    a. Continuity personnel and alternates are accounted for within 12 hours of activation.
    b. All other employees within the affected area are accounted for within five (5) days after activation of an organization's continuity plan.

c. Accountability of personnel is reported to FEMA via the CSR daily until 100% accountability is achieved.

2. Performing essential functions.
3. Establishing communications with supporting and supported organizations and other stakeholders.
4. Preparing for the reconstitution of the organization.

Reconstitution Phase

Leadership communicates instructions for resumption of normal operations to all staff, and supervises an orderly return to the normal operating facility, moving to another temporary facility, or moving to a new permanent facility. The process of reconstitution will generally start immediately after an event concludes.

Some of the activities involved with reconstitution include:

1. Assessing the status of the affected facility or facilities;
2. Determining how much time is needed to repair the affected facility and/or to acquire a new facility;
3. Supervising facility repairs;
4. Notifying decision makers of the status of repairs, including estimates of when the repairs will be completed; and,
5. Implementing a priority-based, phased approach to reconstitution.

Organizational HQs submit a RSR providing initial, monthly, and final status of reconstitution efforts of the organization as it transitions back to normal operations. The RSR provides a real-time view of the organization's reconstitution status during an event.

For assistance with the submission of the RSR, contact the RRS Team by email at rrs-submission@fema.dhs.gov.

Requirements and Criteria for Operational Phases and Implementation:

At a minimum, organizations must do the following when implementing their continuity plans and procedures:

1. Organization HQ must submit continuity readiness status information via RRS no later than the monthly deadline set by FEMA NCP.
2. Follow procedures for plan implementation, including using a decision matrix for continuity plan activation.
3. Alert and notify the following of continuity plan activation:
    a. All continuity personnel;
    b. Alternate location personnel and on-site support teams;
    c. Interdependent agencies; and,
    d. Other points-of-contact, stakeholders, and vendors.

4. Report changes to continuity activation status, or capacity to sustain essential functions.
    a. Non-HQ organizations must notify their HQ upon activation of continuity plans, if possible.
    b. Upon activation of continuity plans at any level or location, organization HQ POCs must notify FEMA and submit a CSR on continuity activities as appropriate; the form and procedures used will be provided by FEMA NCP at the time of execution or activation of call-down procedures. FEMA will collate this information into the RRS. For assistance and additional guidance on reporting, contact the RRS Team by email at rrs-submission@fema.dhs.gov.
5. Follow procedures for the relocation of ERG members and essential records to alternate locations and/or activation of devolution sites.
6. Utilize drive-away kits, as applicable.
7. Conduct in-processing, reception, and accountability of ERG members at the alternate site or of DERG members at the devolution site.
8. Transition responsibilities from the primary operating facility to deployed ERG members at the alternate site or to DERG members at the devolution site.
9. Account for personnel:
    a. Continuity personnel and alternates must be accounted for within 12 hours of activation.
    b. All other employees within the affected area must be accounted for within five (5) days after activation of an organization's continuity plan.
    c. Accountability of personnel will be reported to FEMA via the CSR daily until 100% accountability is achieved.
10. Communicate instructions and operating status with all personnel before, during, and after the continuity event.
11. Utilize human resources guidance for emergencies, as needed, to assist the organization in continuing essential functions.
12. Provide guidance to non-continuity personnel.
13. Identify and alert replacement personnel, as necessary.
14. Organizations must have the capability for continuity personnel to be fully operational at the alternate facility as soon as possible but no later than 12 hours after a continuity activation, and to sustain operations for a minimum of 30 days or until normal operations are resumed. This capability must include:
    a. Sufficient quantity and mode/media of interoperable and available redundant and survivable communication capabilities to enable performance of essential functions;
    b. Capabilities to access and use essential records necessary to facilitate the performance of essential functions, to include having the appropriate media for accessing essential records;

c. Sufficient levels of physical security to protect against all threats identified in the continuity facility's risk assessment; and,

d. Sufficient levels of information security to protect against all threats identified in the continuity facility's risk assessment.

15. Procure necessary equipment and supplies to support and continue performance of essential functions and sustain operations that are not already in place.
16. Comply with any additional continuity reporting requirements from FEMA.
17. Identify all available organization leadership at the alternate locations and conduct the orderly and pre-defined transition of leadership for the position of Organization Head, as well as for key supporting positions, in accordance with orders of succession and delegations of authority, as applicable.
18. Coordinate with GSA for support in acquiring, equipping, and sustaining an appropriate reconstitution site based on the following:
    a. Total office area square footage required to accommodate staff;
    b. Special needs space (e.g., labs, classified facilities);
    c. Equipment and IT needs; and,
    d. Configuration of space (e.g., work areas, conference rooms).
19. Assess the status of affected facilities, determine how much time is needed to repair the affected facility and/or acquire a new facility, supervise facility repairs, and notify organizational leadership of the status of repairs, including estimates of when the repairs will be completed.
20. Verify that all systems, communications, and other required capabilities are available and operational at the new or restored primary operating facility and that the organization is fully capable of performing essential functions and operations at the new or restored primary operating facility.
21. Inform personnel that the actual incident, or threat, no longer exists and instruct personnel on how to resume normal operations.
22. Conduct a smooth transition from the continuity facility to either the normal operating facility, another temporary facility, or a new permanent primary operating facility.
23. Determine which (if any) records were affected by the incident and ensure an effective transition or recovery of essential records and databases, as well as other records that had not been designated as essential records.
24. Promptly report any unlawful or accidental removal, defacing, alteration, or destruction of records in the custody of that agency to NARA, Modern Records Programs, 8601 Adelphi Road, College Park, MD 20740-6001, (301) 837-1738. (*Source: CFR 32, § 1230.14*). The report must include:
    a. A complete description of the records with volume and dates, if known;
    b. The name of the office maintaining the records;

c. A statement of the exact circumstances surrounding the removal, defacing, alteration, or destruction of records;

d. A statement of the safeguards established to prevent further loss of documentation; and,

e. When appropriate, details of the actions taken to salvage, retrieve, or reconstruct the records.

25. Report reconstitution status to FEMA NCP via the RRS.

a. Submit Reconstitution Status Report, as required, using the procedures provided by FEMA NCP at the time of execution.

b. Contact FEMA NCP at rrs-submission@fema.dhs.gov for assistance and additional guidance on reporting procedures.

ANNEX M: ACRONYMS

AAR	After-Action Report
BIA	Business Impact Analysis
BPA	Business Process Analysis
CAG	Continuity Advisory Group
COG	Continuity of Government
COGCON	Continuity of Government Readiness Conditions
COOP	Continuity of Operations
CRC	Continuity Readiness Cell
CSR	Continuity Status Report
CWG	Continuity Working Group
DHS	U.S. Department of Homeland Security
DERG	Devolution Emergency Response Group
ERG	Emergency Relocation Group
ESA	Essential Supporting Activity
FCD	Federal Continuity Directive
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act
GETS	Government Emergency Telecommunications Service
GSA	U.S. General Services Administration
HQ	Headquarters
HSEEP	Homeland Security Exercise and Evaluation Program
ICWG	Interagency Continuity Working Group
IP	Improvement Plan
ISCP	Information System Contingency Plan
IT	Information Technology
MEF	Mission Essential Function
MOA/MOU	Memorandum of Agreement/Memorandum of Understanding
MYSPMP	Multi-Year Strategy and Program Management Plan
NARA	National Archives and Records Administration
NCC	National Continuity Coordinator
NCP	National Continuity Programs
NED	National Exercise Division
NEF	National Essential Function
NIST	National Institute of Standards and Technology
OEP	Occupant Emergency Plan
OMB	Office of Management and Budget
OPSEC	Operations Security
OPM	U.S. Office of Personnel Management
OSTP	Office of Science and Technology Policy
PMEF	Primary Mission Essential Function
POC	Point of Contact
PPD	Presidential Policy Directive
QL/CSR	Quick Look/Continuity Status Report

RRS	Readiness Reporting System
RSR	Reconstitution Status Report
SAC COOPC	Small Agency Council Continuity of Operations Committee
SF	Standard Form
SLTT	State, local, territorial, and tribal
TSP	Telecommunications Service Priority
TT&E	Test, Training, and Exercise
U.S.C.	United States Code
WPS	Wireless Priority Service

ANNEX N: DEFINITIONS

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

Agencies – Departments and agency (D/As) are those executive departments enumerated in 5 U.S.C. § 101 and independent establishments as defined by 5 U.S.C. § 104(1), Government corporations as defined by 5 U.S.C. § 103(1), and the United States Postal Service. D/As, commissions, bureaus, boards, and independent organizations are referred to in this document as "organizations."

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

Alternate Locations – Fixed, mobile, or transportable locations, other than the headquarters facility, where D/A leadership and continuity personnel relocate in order to perform essential functions following activation of the continuity plan. These include locations to which agency leadership may devolve. These locations refer to not only locations sites but also work arrangements such as telework and mobile work.

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

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

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.

Category – Refers to the categories of D/As listed in PPD-40, Annex A.

Cold Site – A facility that is neither staffed nor operational on a daily basis. Telecommunications, IT equipment, and infrastructure is typically present at the location, however teams of specialized personnel must be deployed to activate the systems before the site can become operational. Basic infrastructure and environmental controls are present (e.g., electrical and heating, ventilation and air conditioning systems), yet systems are not continuously active.

Communications – Voice, video, and data capabilities that enable organizational leadership and staff to assure 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 the ability to communicate internally and with other entities (including with other Federal organizations, SLTT governments, and the private sector) as necessary to perform essential functions.

Component – A sub-organization or directorate that supports HQ leadership in the performance of PMEFs and/or MEFs, by performing those MEFs and/or ESAs required to complete a PMEF or NEF. Examples of a component could be an agency, bureau, regional office, district office, and/or a local office.

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

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

Continuity Capability – The ability of an organization to continue to perform its essential functions, using COOP and Continuity of Government (COG) programs and continuity requirements that have been integrated into the organization's daily operations. The primary goal is preserving of our form of government under the U.S. Constitution and the continued performance of NEFs under all conditions. Building upon a foundation of continuity planning and continuity program management, the pillars of a continuity capability are: leadership, staff, communications, and facilities.

Continuity Coordinators – Senior accountable Executive Branch officials at the Assistant Secretary or equivalent level who represent their D/as on the CAG, ensure continuity capabilities in the organization, and provide recommendations for continuity policy. Continuity Coordinators are supported primarily by the Continuity Manager and by other continuity planners or coordinators at their subordinate levels throughout their organizations.

Continuity of Government (COG) – A coordinated effort within the executive, legislative, or judicial branches of the Federal Government to ensure that NEFs continue to be performed during a catastrophic emergency.

Continuity of Government Readiness Conditions (COGCON) – The COGCON system establishes executive continuity program readiness levels, focusing on emergencies in or credible threats to the National Capital Region, or affecting the performance of NEFs.

Continuity of Operations (COOP) – An effort within the Executive Office of the President and individual D/As to ensure that essential functions continue to be performed during disruption of normal operations.

Continuity Manager – The Senior Continuity Planner responsible for managing day-to-day continuity programs, representing his/her D/A on the Continuity Advisory Group and working groups, as appropriate, and reporting to the Continuity Coordinator on all continuity program activities.

Continuity Personnel – Those personnel, both senior and core, who provide organizational leadership with advice, recommendations, and functional support necessary to continue essential functions during continuity operations. Continuity personnel are referred to as ERG or DERG members.

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

Continuity Program Management Cycle – An ongoing, cyclical model of planning, training, evaluating, and implementing corrective actions for continuity capabilities.

Corrective Action Program (CAP) – An organized method of documenting and tracking improvement actions for an organization's continuity program.

Critical Asset – An asset of such strategic importance to the performance of essential functions that its incapacitation or destruction would have a very serious or debilitating effect on an organization's ability to perform the function(s).

Critical Infrastructure (CI) – Defined in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), 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 national economic security, national public health and safety, or a combination thereof.

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

Devolution Emergency Response Group (DERG) – Personnel stationed at a geographically dispersed location, other than the primary location, who are identified to continue performance of essential functions.

Diversity – Distributed or expanded among various types or forms. For example, communications system route diversity is communications routing between two points over more than one geographic or physical path with no common points.

Drive-Away Kit – A kit prepared by, and for, an individual who expects to deploy to an alternate location during an emergency. The kit contains items needed to minimally satisfy an individual's personal and professional needs during deployment, such as clothing, medications, a laptop, and other necessities.

Emergency Operating Records – Those types of vital records essential to the continued functioning or reconstitution of an organization during and after an emergency. They include emergency plans and directive(s), orders of succession, delegations of authority, staffing assignments, and selected program records needed to continue the most critical agency operations, as well as related policy or procedural records that assist agency staff in conducting operations under emergency conditions and for resuming normal operations after an emergency.

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

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

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.

Essential Functions – A subset of government functions that are determined to be critical activities. These essential functions are then used to identify supporting tasks and resources that must be included in the organization's continuity planning process. In this FCD, the term "essential functions" refers to those functions an organization must continue in a continuity situation, whether the functions are MEFs, PMEFs, or ESAs.

Essential Records – Information systems and applications, electronic and hardcopy documents, references, and records needed to support essential functions during a continuity event. The two basic categories of essential records are emergency operating records and rights and interest records. Emergency operating records are essential to the continued functioning or reconstitution of an organization. Rights and interest records are critical to carrying out an organization's essential legal and financial functions and vital to the protection of the legal and financial rights of individuals who are directly affected by that organization's activities. The term "vital records" refers to a specific sub-set of essential records relating to birth, death, and marriage documents.

Essential Records Packet – An electronic or hardcopy compilation of key information, instructions, and supporting documentation needed to access essential records in an emergency situation.

Essential Supporting Activities (ESAs) – Critical functions that an organization must continue during a continuity activation, but that do not meet the threshold for MEFs or PMEFs.

Executive Branch Department and Agencies (D/As) – The Executive Branch departments and agencies 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), Intelligence agencies as defined by 50 U.S.C. 3003, and the United States Postal Service. These D/As are referred to as "organizations" throughout this FCD.

Federal Continuity Directive (FCD) – A document developed and promulgated by DHS/FEMA, in coordination with the Continuity Advisory Group and in consultation with the Continuity Policy Coordination Committee, which directs Executive Branch organizations to carry out identified continuity planning requirements and assessment criteria.

Geographic Dispersion – The distribution of personnel, functions, facilities, and other resources in physically different locations from one another.

Government Functions – Government functions are the collective functions the Executive Office of the President and D/As as defined by statute, regulation, presidential direction, or other legal authority, to include the functions of the legislative and judicial branches.

Headquarters (HQ) – In this FCD, the term "headquarters" refers to the central or head offices for operations of organizations identified in PPD-40, Annex A.

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

Hot Site – Hot sites are locations that operate 24 hours a day with fully operational equipment and capacity to immediately assume operations upon loss of the primary facility. A hot continuity facility requires on-site telecommunications, information, infrastructure, equipment, back-up data repositories, and personnel required to sustain essential functions.

Interagency Agreement (IAA) – A written agreement entered into between two Federal agencies, or major organizational units within an agency, which specifies the goods to be furnished or tasks to be accomplished by one agency (the servicing agency) in support of the other (the requesting agency).

Interagency Board – A working group established by the NCC to review and recommend potential PMEFs submitted by organizations before they are submitted to the NCC for final approval.

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 so 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.

Leadership – The senior decision makers who have been elected (e.g., President, Governors) or designated (e.g., Cabinet Secretaries, Administrators) to head government organizations. Depending on the organization, directors and managers may also serve in guiding the organization and making decisions.

Legal and Financial Rights Records – Vital records essential to protect the legal and financial rights of the government and the individuals directly affected by its activities. Examples include accounts receivable records, social security records, payroll records, retirement records, and insurance records. These records were formerly defined as ‘‘rights-and-interests’’ records.

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

Mission Essential Functions (MEFs) – The essential functions directly related to accomplishing an organization’s mission as set forth in statutory or executive charter. Generally, MEFs are unique to each organization.

Multi-Year Strategy and Program Management Plan (MYSPMP) – A plan that guides the development of the organization’s continuity program over a set number of years via a process that ensures the maintenance and continued viability of continuity plans.

National Capital Region (NCR) – The National Capital Region was created pursuant to the National Capital Planning Act of 1952 (40 U.S.C. § 71). The Act defined the NCR as the District of Columbia; Montgomery and Prince George’s Counties of Maryland; Arlington, Fairfax, Loudoun, and Prince William Counties of Virginia; and all cities now or hereafter

existing in Maryland or Virginia within the geographic area bounded by the outer boundaries of the combined area of said counties. The NCR includes the District of Columbia and 11 local jurisdictions in the State of Maryland and the Commonwealth of Virginia.

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

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

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

National Exercise Program (NEP) – The NEP serves as the principal exercise mechanism for examining and measuring the preparedness and readiness of the United States. This includes designing, coordinating, conducting, and evaluating a progressive cycle of exercises that rigorously test the Nation's ability to perform missions or functions that prevent, protect against, respond to, recover from, and mitigate all hazards.

Normal Operations – Refers to the broad functions undertaken by an organization; these functions include day-to-day tasks, planning, and execution of tasks. May also be referred to as steady-state operations.

Occupant Emergency Plan (OEP) – A short-term emergency response plan which establishes procedures for evacuating buildings or sheltering-in-place to safeguard lives and property. Organizations may refer to this plan as the Emergency Plan or Building Closure Plan. Common scenarios that would lead to the activation of these plans include inclement weather, fire, localized power outages, and localized communications outages. These types of events are generally short-term in nature.

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.

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 towards accomplishing one or more objectives or goals.

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

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

Program – A group of related initiatives managed in a coordinated process so as to obtain a level of control and benefits that would not be possible from the individual management of the initiatives. Programs may include elements of related work outside the scope of the discrete initiatives within the program.

Readiness Reporting System (RRS) – A DHS/FEMA program that collects and manages continuity capability data and assessments of the ability of executive branch organizations to perform their PMEFs in support of the NEFs. The RRS supports analysis and tracks capabilities at all times under all conditions, to include natural disasters, manmade incidents, terrorism, and war.

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

Recovery – The implementation of prioritized actions required to return an organization's processes and support functions to operational stability following a change in normal operations.

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

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

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

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

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

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

Small Agency Council Continuity of Operations Committee (SAC COOPC) – Provides a forum for the development and integration of continuity policies and programs among the Federal Government organizations represented on the Committee. DHS/FEMA provides assistance to the SAC COOPC as requested by the SAC COOPC Chair.

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 D/A 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.

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

Telework Site – An approved worksite where an employee performs his or her duties other than the location from which the employee would otherwise work.

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

Vital Records – See Essential Records.

Warm Site – Locations that have a minimum acceptable level of infrastructure in-place, and also possess the IT and telecommunications equipment to become operational as soon as possible, but not later than 12 hours after continuity activation. In order to become active, a warm facility requires additional personnel, equipment, supplies, software, or customization. Warm sites generally possess the resources necessary to sustain critical mission/business processes, but lack the capacity to activate all systems or components.

ANNEX O: AUTHORITIES AND RESOURCES

AUTHORITIES

1) Homeland Security Act of 2002, as amended (6 U.S.C. § 101 *et seq.*).
2) National Security Act of 1947, as amended (50 U.S.C. § 3042).
3) Telework Enhancement Act of 2010 (5 U.S.C. §§ 6501-6506).
4) Executive Order 12148, *Federal Emergency Management*, July 20, 1979, as amended.
5) Executive Order 13618. *Assignment of National Security and Emergency Preparedness Communications Functions*, July 6, 2012.
6) Presidential Policy Directive 8, *National Preparedness*, March 30, 2011.
7) Presidential Policy Directive, 40, *National Continuity Policy*, July 15, 2016.
8) Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, February 12, 2013.
9) Vacancies Reform Act of 1998, as amended (5 U.S.C. §§ 3345-3349d).

RESOURCES

1) 36 Code of Federal Regulations, Part 1223, *Managing Vital Records*.
2) 36 Code of Federal Regulations, Part 1236, *Electronic Records Management*.
3) 44 Code of Federal Regulations, Part 3541, *Federal Information Security Management Act of 2002*.
4) FCD-2, *Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process*, July 2013.
5) Homeland Security Exercise and Evaluation Program (HSEEP), April 2013.
6) Intelligence Community Standard Number 500-19, *Universal Access and Remote Access to TS/SCI Web Content and Services*, July 7, 2010.
7) National Institute of Standards and Technology, Special Publication 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.
8) Office of Management and Budget Memorandum M-05-16, *Regulation on Maintaining Telecommunication Services during a Crisis or Emergency in Federally-owned Buildings*, June 30, 2005.
9) *OPM Guide to Telework in the Federal Government*, April 2011.
10) *OPM Washington, DC, Area Dismissal and Closure Procedures*, December 2015.
11) *OPM Handbook on Pay and Leave Benefits for Federal Employees Affected by Severe Weather Conditions or Other Emergency Situations*, June 2008.
12) *OPM Human Resources Flexibilities and Authorities in the Federal Government*, August 2013.
13) National Exercise Program Implementation Plan, June 2013.

14) National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.

15) National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Recommended Security Controls for Federal Systems and Organizations*, August 2013.

16) National Preparedness Goal, September 2015.

17) Risk Resources (select):

a. National Infrastructure Protection Plan (NIPP), 2013.

b. NIPP Supplemental Tool: *Executing a Critical Infrastructure Risk Management Approach.*

c. National Institute of Standards and Technology, Special Publication 800-30, Rev 1, *Guide for Conducting Risk Assessments*, September 2012.

d. National Institute of Standards and Technology, Special Publication 800-39, *Managing Information Security Risk Organization, Mission, and Information System View*, March 2011.

e. *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard,* August 2013, 1st Edition.