



Federal Continuity Directive 1

Federal Executive Branch National Continuity Program and Requirements

October 2012



**Homeland
Security**



**Homeland
Security**

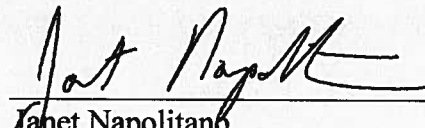
This page is intentionally blank.

In May 2007, the National Security Presidential Directive-51/Homeland Security Presidential Directive-20, *National Continuity Policy*, was issued by the President to establish and maintain a comprehensive and effective national continuity capability to ensure resilience and the preservation of our form of Government under the Constitution and the continuing performance of National Essential Functions under all conditions. In August 2007, the President approved the *National Continuity Policy Implementation Plan* to build upon the *National Continuity Policy* and provide guidance to Federal Executive Branch organizations on appropriately identifying and carrying out their Primary Mission Essential Functions that support the eight National Essential Functions—the most critical functions necessary to lead and sustain the Nation during a catastrophic emergency.

To provide the operational guidance to implement this policy, the Department of Homeland Security, in coordination with its interagency partners, developed *Federal Continuity Directive (FCD) 1*, dated February 2008. In this update to the FCD, new policies and clarifications to existing policies are provided to give direction for the further development of continuity plans and programs for the Federal Executive Branch. Effective continuity planning and programs enhance the resilience of organizations and facilitate the performance of essential functions during all-hazards emergencies or other situations that may disrupt normal operations. The primary goal of continuity in the executive branch is the continuation of essential functions.

In this directive, the elements of a viable continuity capability for our Nation are discussed. These elements, along with the coordination of tribal, state, territorial, and local governments and the private sector, are critical to establishing and maintaining a comprehensive and effective continuity capability. Continuity programs and operations are simply good business practices that ensure government functions and services will be available to the Nation's citizens under all conditions.

The provisions of this FCD are applicable at all levels of Federal Executive Branch organizations regardless of their location, including regional and field locations.



Janet Napolitano
Secretary of Homeland Security

This page is intentionally blank.

TABLE OF CONTENTS

1.	PURPOSE	1
2.	APPLICABILITY AND SCOPE	1
3.	SUPERSESSION	1
4.	AUTHORITIES.....	1
5.	REFERENCES	1
6.	POLICY.....	2
7.	BACKGROUND.....	2
8.	PROGRAM MANAGEMENT	3
9.	ELEMENTS OF A VIABLE CONTINUITY CAPABILITY	5
10.	COORDINATION WITH TRIBAL, STATE, TERRITORIAL, AND LOCAL GOVERNMENTS AND THE PRIVATE SECTOR	8
11.	CONTINUITY PLAN OPERATIONAL PHASES AND IMPLEMENTATION.....	9
12.	ROLES AND RESPONSIBILITIES.....	10
13.	POINT OF CONTACT	10
14.	DISTRIBUTION	10
ANNEX A.	PROGRAM PLANS AND PROCEDURES	A-1
ANNEX B.	RISK MANAGEMENT.....	B-1
ANNEX C.	BUDGETING AND ACQUISITION OF RESOURCES.....	C-1
ANNEX D.	ESSENTIAL FUNCTIONS.....	D-1
ANNEX E.	ORDERS OF SUCCESSION	E-1
ANNEX F.	DELEGATIONS OF AUTHORITY	F-1
ANNEX G.	CONTINUITY FACILITIES.....	G-1
ANNEX H.	CONTINUITY COMMUNICATIONS.....	H-1
ANNEX I.	ESSENTIAL RECORDS MANAGEMENT	I-1
ANNEX J.	HUMAN RESOURCES	J-1
ANNEX K.	TEST, TRAINING, AND EXERCISE (TT&E) PROGRAM	K-1
ANNEX L.	DEVOLUTION OF CONTROL AND DIRECTION	L-1
ANNEX M.	RECONSTITUTION OPERATIONS	M-1
ANNEX N.	CONTINUITY PLAN OPERATIONAL PHASES AND IMPLEMENTATION.....	N-1
ANNEX O.	ACRONYMS.....	O-1
ANNEX P.	GLOSSARY	P-1
ANNEX Q.	AUTHORITIES AND REFERENCES	Q-1

This page is intentionally blank.



FEDERAL CONTINUITY DIRECTIVE 1

Number	Date	Office
FCD 1	2012	FEMA National Continuity Programs

TO: HEADS OF FEDERAL ORGANIZATIONS

SUBJECT: FEDERAL EXECUTIVE BRANCH NATIONAL CONTINUITY PROGRAM AND REQUIREMENTS

- 1. PURPOSE:** This Federal Continuity Directive (FCD) provides direction to the Federal Executive Branch for developing continuity plans and programs. Continuity planning facilitates the performance of executive branch essential functions during all-hazards emergencies or other situations that may disrupt normal operations. The ultimate goal of continuity in the executive branch is the continuation of National Essential Functions (NEFs).
- 2. APPLICABILITY AND SCOPE:** In accordance with National Security Presidential Directive (NSPD)-51/Homeland Security Presidential Directive (HSPD)-20, *National Continuity Policy*, the provisions of this FCD are applicable to the executive departments enumerated in 5 U.S.C. § 101, including the 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 departments, agencies, commissions, bureaus, boards, and independent organizations are hereinafter referred to as “organizations” to better reflect the diverse organizational structures of the Federal Executive Branch. The provisions of this FCD are applicable at all levels of Federal Executive Branch organizations regardless of their location, including regional and field locations. Headquarters (HQ) organizations 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 Annex A of NSPD-51/HSPD-20. The Federal Emergency Management Agency (FEMA) has developed Continuity Guidance Circulars 1 and 2 to provide similar guidance to tribal, state, territorial, and local governments and the private sector.
- 3. SUPERSESSSION:** The provisions of this FCD supersede Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements*, dated February 2008.
- 4. AUTHORITIES:** See Annex Q – Authorities and References.
- 5. REFERENCES:** See Annex Q – Authorities and References.

- 6. POLICY:** It is the policy of the United States to maintain a comprehensive and effective continuity capability composed of Continuity of Operations (COOP) and Continuity of Government (COG) programs to ensure the preservation of our form of Government under the Constitution and the continuing performance of NEFs under all conditions. All organizations must incorporate continuity requirements into their daily operations to ensure seamless and immediate continuation of Primary Mission Essential Functions (PMEFs) so that essential functions and services remain available to the Nation’s citizens. Continuity planning will occur simultaneously with the development and execution of day-to-day organizational programs. This means that organizations must incorporate redundancy and resiliency as a means and an end. In support of this policy, the Federal Executive Branch has developed and implemented a continuity program that is composed of programs within individual organizations to ensure that they can continue to perform their essential functions during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies. These efforts include plans and procedures under all readiness levels that delineate essential functions, specify succession to office and delegations of authority, provide for the safekeeping of and access to essential records, identify a range of continuity facilities, provide for continuity communications, provide for human resources planning, validate these capabilities through tests, training, and exercises (TT&E), specify a devolution of control and direction, and provide for reconstitution. All Federal Executive Branch organizations, regardless of their size or location, shall have in place a viable continuity capability to ensure resiliency and continued performance of their organization’s essential functions under all conditions.
- 7. BACKGROUND:** Continuity planning is simply the good business practice of ensuring the execution of essential functions through all circumstances, and it is a fundamental responsibility of public and private entities responsible to their stakeholders. Today’s threat environment and the potential for no-notice emergencies, including localized acts of nature, accidents, technological emergencies, and military or terrorist attack-related incidents, have increased the need for robust continuity capabilities and planning that enable organizations to continue their essential functions across a broad spectrum of emergencies. Today’s threats have emphasized the importance of programs that ensure continuity throughout the Federal Executive Branch.

Historically, the Federal Government has defined continuity efforts using the terms “COOP,” “COG,” and “Enduring Constitutional Government (ECG).”

"COOP," or **Continuity of Operations**, is an effort within *individual* organizations (i.e., Federal executive branch organizations) to ensure that MEFs and PMEFs continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.

"COG," or **Continuity of Government**, means a *coordinated* effort within each branch of Government (e.g., the Federal Government's executive branch) to ensure that NEFs continue to be performed during a catastrophic emergency.

"ECG," or **Enduring Constitutional Government**, means a *cooperative* effort among the legislative, executive, and judicial branches of the Federal Government, coordinated by the President, as a matter of comity with respect to the legislative and judicial branches and with proper respect for the constitutional separation of powers among the branches, to preserve the constitutional framework under which the Nation is governed and the capability of all three branches of government to execute their constitutional responsibilities and provide for orderly succession, appropriate transition of leadership, interoperability, and support of NEFs during a catastrophic emergency.

Figure 1

The lessons we have learned from such catastrophic events as the attacks of September 11, 2001, and Hurricane Katrina in 2005 demonstrate the need to reemphasize continuity as a “good business practice” to be incorporated into day-to-day planning, in order to reduce vulnerability and ensure continuity.

On May 4, 2007, the President issued the *National Continuity Policy* in NSPD-51/HSPD-20, which set forth a new vision to ensure the continuity of our Government. Pursuant to NSPD-51/HSPD-20, and in accordance with the National Continuity Policy Implementation Plan (NCPIP), the President directs the executive branch to reorient itself and to utilize an integrated, overlapping national continuity concept to ensure the preservation of our Government and the continuing performance of essential functions.

Continuity responsibility and planning should not be a separate and compartmentalized function performed by independent cells of a few planners in each organization. Organizations must fully integrate continuity into all aspects of an organization’s daily operations, thus creating a “culture of continuity.”

- 8. PROGRAM MANAGEMENT:** The NCPIP recognizes that an organization’s resiliency is directly related to its continuity capability. An organization’s continuity capability – its ability to perform its essential functions continuously – rests upon key components and pillars. These pillars are leadership, staff, communications, and facilities.

The key pillars are built on the foundation of continuity planning and program management. A standardized continuity program management cycle ensures consistency across all Federal Government continuity programs. The cycle establishes consistent performance metrics, promulgates best practices, and facilitates consistent cross-organization continuity evaluations. Organizations should use this continuity program management cycle to develop and implement their continuity programs.

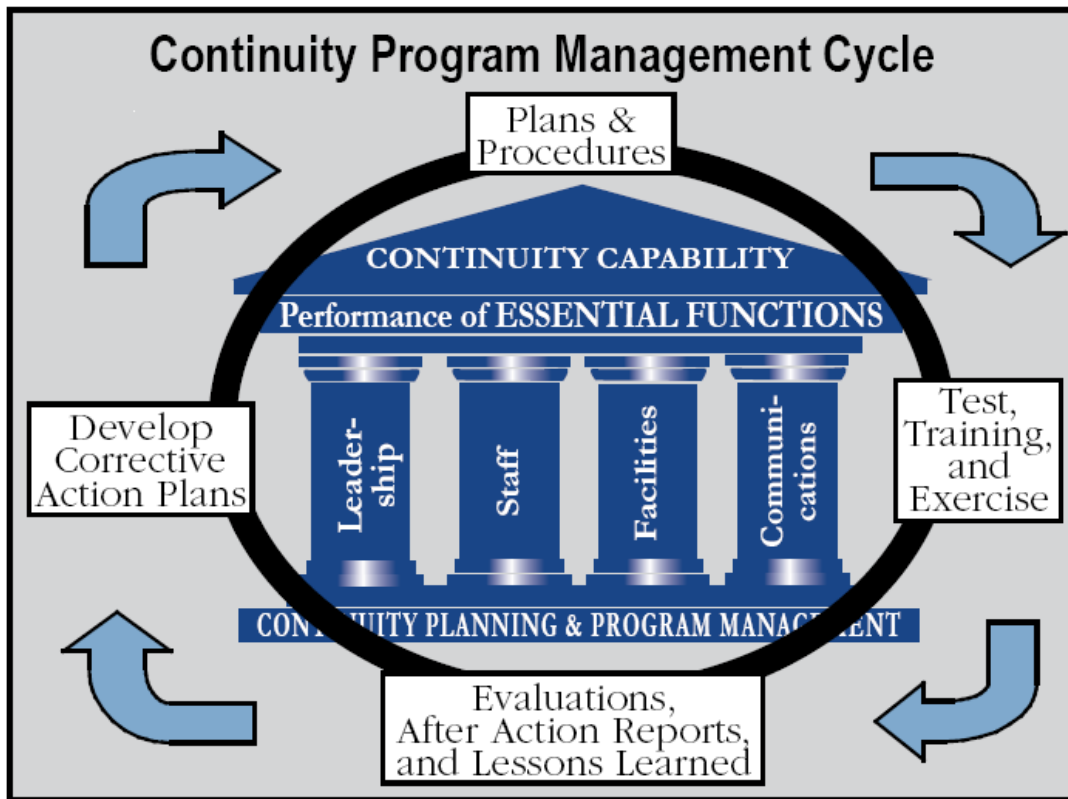


Figure 2

See Annex A – Program Plans and Procedures

Risk Management

In the face of multiple and diverse catastrophic possibilities, it is accepted that risk is a permanent condition. Risk management is 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. It is a responsibility of Government to ensure that essential services can continue regardless of whether organizations have adequately mitigated risks. Applying a disciplined approach to managing risk will help to achieve best progress, long term success, and overall effectiveness and efficiency. Organizations manage their internal risks to a reasonable level, employing risk management principles to identify and prioritize risks based on perceived loss or impact associated with each. Organizations should discuss all risks with senior organization leadership to determine an agreed upon course of action to correct and contain risks to an acceptable level.

See Annex B – Risk Management

Budgeting

Budgeting for and acquiring resources for continuity capabilities is one of the most important components of continuity planning. Budgetary requirements directly support the ability of all organizations to meet all the criteria of a viable continuity capability as stated in this FCD.

See Annex C – Budgeting and Acquisition of Resources

9. ELEMENTS OF A VIABLE CONTINUITY CAPABILITY: NSPD-51/HSPD-20

outlines the overarching continuity requirements for organizations. These requirements are discussed in more depth in the “Key Considerations and Concept of Operations” section of the NCPIP. These components are further delineated into the following elements of continuity.

a. **ESSENTIAL FUNCTIONS**. The identification and prioritization of essential functions is a prerequisite for continuity planning, because they establish the planning parameters that drive an organization’s efforts in all other planning and preparedness areas.

Government functions are the collective functions of organizations, as defined by the Constitution, statute, regulation, Presidential direction, or other legal authorities, and the functions of the legislative and judicial branches. These functions are activities that are conducted to accomplish an organization’s mission and serve its stakeholders. During an event that disrupts or has the potential to disrupt normal activities and that necessitates the activation of continuity plans, the resources and staff available to an organization will likely be limited, and the organization will not be able to perform all of its normal government functions. Therefore, a subset of those government functions that are determined to be critical activities are defined as the organization’s essential functions. These essential functions are used to identify supporting tasks and resources that must be included in the organization’s continuity planning process. FCD 2 provides additional details and procedures for identifying an organization’s essential functions.

The NCPIP identifies three categories of essential functions: NEFs, PMEFS, and Mission Essential Functions (MEFs). The ultimate goal of continuity in the executive branch is the continuation of NEFs. To achieve that goal, the objective for executive organizations is to identify their MEFs and PMEFS, as appropriate, and ensure that those functions can be continued throughout, or resumed rapidly after, a disruption of normal activities.

The eight NEFs represent the overarching responsibilities of the Federal Government to lead and sustain the Nation and are the primary focus of the Federal Government’s leadership during and in the aftermath of an emergency.

PMEFS are the set of those organization essential functions that organizations must perform to support or implement the performance of the NEFs before, during, and in the aftermath of an emergency. Organizations need to continuously perform PMEFS during a continuity activation or resume PMEFS within 12 hours of an event. Organizations must maintain all PMEFS until they can resume normal operations.

MEFs are a broader set of essential functions that organizations must continue throughout or resume rapidly after a disruption of normal activities but are not identified as PMEFs. MEFs are those functions that enable an organization to provide vital services, exercise civil authority, maintain the safety of the public, and sustain the industrial/economic base.

In addition, organizations may identify functions that the organization must continue in a continuity activation, but that are not recognized as PMEFs or MEFs, such as human resources management, security, and facilities management. These functions remain essential and are denoted as Essential Supporting Activities. In this FCD, the term “essential functions” refers to those functions an organization must continue in a continuity activation, whether the functions are MEFs, PMEFs, or Essential Supporting Activities.

See Annex D – Essential Functions

b. ORDERS OF SUCCESSION. Organizations are responsible for establishing, promulgating, and maintaining orders of succession to key positions. Such orders of succession are essential to ensure that the organization has clearly established and identified leadership and key personnel, if these leaders are incapacitated or otherwise unavailable.

See Annex E – Orders of Succession

c. DELEGATIONS OF AUTHORITY. Delegation of authorities for making policy determinations and for taking necessary actions at all levels of an organization ensures a rapid and effective response to any emergency requiring the activation of a continuity plan. It is vital to clearly establish delegations of authority so that all organization personnel know who has legal authorization to make key decisions and take necessary actions during continuity activation and operations. Generally, a predetermined delegation of authority will take effect when normal channels of direction and control are disrupted and will lapse when those channels are reestablished.

See Annex F – Delegations of Authority

d. CONTINUITY FACILITIES. The use of continuity facilities enhances the resiliency and continuity capability of organizations. The term “continuity facilities” is comprehensive, referring to both alternate and devolution sites where essential functions are continued or resumed during a continuity event. “Alternate sites” are locations, other than the primary facility, used to carry out essential functions, usually by relocating Emergency Relocation Group (ERG) members following activation of the continuity plan. “Devolution sites” are locations used to carry out essential functions by devolving the essential functions to a geographically-separated facility and staff following activation of the devolution plan. These sites refer to not only other facilities and locations, but also work arrangements such as telework and mobile work concepts.

See Annex G – Continuity Facilities

e. CONTINUITY COMMUNICATIONS. The ability of an organization to execute its essential functions at its continuity facilities depends on the identification, availability, reliability, and redundancy of critical secure and non-secure communications and information technology (IT) systems. These communications and systems support connectivity among key government leadership personnel, internal organization elements, other organizations, critical customers, and the public. By mirroring capabilities used during day-to-day operations and choosing resilient communications and IT systems that are capable of operating under conditions that may involve power or other infrastructure disruptions, organizations further ensure the performance of essential functions in emergency situations.

See Annex H – Continuity Communications

f. ESSENTIAL RECORDS MANAGEMENT. Another critical element of a viable continuity plan and program is the identification, protection, and ready 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 essential functions during a continuity activation. Access to and use of these records and systems enable the performance of essential functions and reconstitution to normal operations. To ensure performance of essential functions, organizations pre-position and regularly update these essential records.

See Annex I – Essential Records Management

g. HUMAN RESOURCES. In a continuity activation, organizations will activate continuity personnel, referred to as the Emergency Relocation Group (ERG), and expect them to perform their assigned duties following their organization’s particular plans and procedures. In addition to supporting the human resources needs of continuity personnel, organizations are also responsible for supporting employees who are not designated as ERG personnel, but may also be affected by a continuity event. Procedures and expectations for these employees should be addressed in continuity and emergency plans, such as the Occupant Emergency Plan (OEP). The Telework Enhancement Act of 2010 states that “each executive agency shall incorporate telework into the continuity of operations plans for that agency.” In preparation for emergencies, organizations should have telework policies in place that provide employees with instructions, procedures and expectations.

See Annex J – Human Resources

h. TESTS, TRAINING, AND EXERCISES. An effective TT&E program facilitates the validation of an organization’s continuity capabilities and the Federal Executive Branch’s ability to perform essential functions during any emergency. Training familiarizes leadership and staff with the procedures and tasks they must perform when executing continuity plans and conducting essential functions. Tests and exercises serve to assess and validate all the components of continuity plans, policies, procedures, systems, and facilities used to ensure continuance of essential functions and identify issues for subsequent improvement. All organizations must plan, conduct, and document periodic TT&E events to prepare for all-hazards continuity emergencies and disasters, identify deficiencies, and demonstrate the

viability of their continuity plans and programs. Deficiencies, actions to correct them, and a timeline for remedy are documented in an organization's Corrective Action Program (CAP).

See Annex K – Test, Training, and Exercises

i. DEVOLUTION OF CONTROL AND DIRECTION. Devolution requires the transition of roles and responsibilities for performance of essential functions through pre-authorized delegations of authority and responsibility. The authorities are delegated from an organization's primary operating staff to other employees internal or external to the organization in order to sustain essential functions for an extended period. Personnel stationed at the devolution site who are identified to conduct essential functions are classified as the Devolution Emergency Response Group (DERG). Devolution planning supports overall continuity planning and addresses the full spectrum of threats and all-hazards emergency events that may render an organization's leadership and staff unavailable to support, or incapable of supporting, the execution of the organization's essential functions from either its primary operating facility or its alternate site.

See Annex L – Devolution of Control and Direction

j. RECONSTITUTION. Reconstitution is the process by which surviving and/or replacement organization personnel resume normal organization operations from the original or replacement primary operating facility. 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. In some cases, extensive coordination may be necessary to backfill staff, procure a new operating facility, and re-establish communications, IT infrastructure, and essential records.

See Annex M – Reconstitution Operations

10. COORDINATION WITH TRIBAL, STATE, TERRITORIAL, AND LOCAL GOVERNMENTS AND THE PRIVATE SECTOR: The Federal Government cannot perform its NEFs, prescribed in NSPD-51/HSPD-20, without the robust involvement of all levels of government and the private sector. Tribal, state, territorial, and local governments play an integral role in determining the needs of the public and in ensuring that essential functions (e.g., police and fire services, emergency medical care) continue on a daily basis.

Federal organizations, as applicable and appropriate, will coordinate with tribal, state, territorial, and local governments, regional entities, and private sector owners and operators of the Nation's critical infrastructure (CI). Such collaboration builds relationships and ensures unity of effort. Examples of coordination that federal organizations may undertake include:

1. Collaborating to incorporate capabilities of other entities into the organization's continuity planning and exercise activities to the extent possible;
2. Coordinating on risk assessments to identify hazards relevant to the organization's mission and location where essential functions are located;

3. Partnering with these entities to develop continuity plans that are coordinated to the extent possible;
4. Participating in Continuity Working Groups (CWGs), information sharing, training, and exercises, as appropriate;
5. Coordinating OEPs, shelter-in-place plans, and regional and local evacuation plans;
6. Participating in existing alert and notification networks and credentialing initiatives, as appropriate;
7. Working together to identify interdependencies and ensuring resiliency with critical infrastructure and services at all levels;
8. Coordinating continuity resource and security requirements, as appropriate;
9. Working to augment and strengthen coordination efforts with organizations to include, but not limited to: DHS/FEMA Regional/State-level CWGs, DHS/Office of Infrastructure Protection and the various CI Sector Coordinating Councils and Government Coordinating Councils, and Federal Executive Boards; and
10. Participating in other coordination activities, as appropriate.

11. CONTINUITY PLAN OPERATIONAL PHASES AND IMPLEMENTATION:

A continuity plan is implemented to ensure the continuation or rapid resumption of essential functions during a continuity activation. The development of an executive decision-making process allows for a review of the emergency and a determination of the best course of action based on the organization’s readiness posture. The continuity implementation process includes four phases: readiness and preparedness, activation, continuity operations, and reconstitution. Organizations may implement the four phases as illustrated in Figure 3.

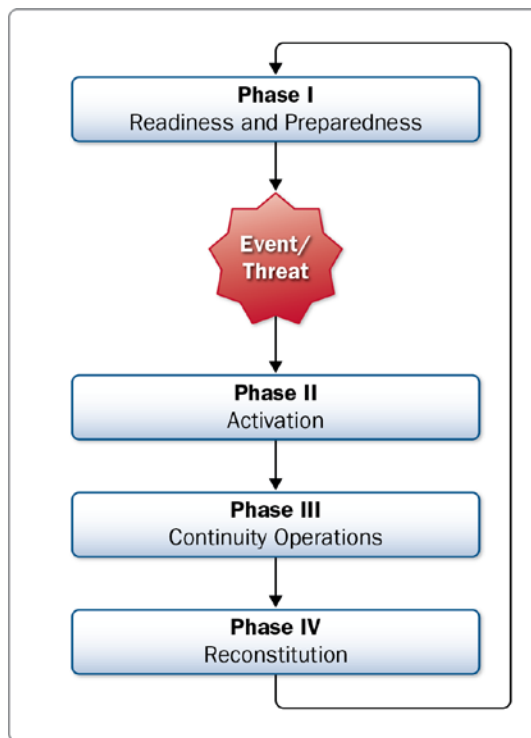


Figure 3

The readiness and preparedness phase includes all organization continuity readiness and preparedness activities including development, review, and revision of plans; TT&E; and risk management. The activation phase includes the activation of organizational continuity plans and all associated procedures necessary to support the continued performance of essential functions. While some personnel may have to relocate to continue essential functions, geographic dispersion also assists organizations in ensuring redundancy and resiliency. The continuity operations phase includes activities to continue essential functions, including communicating with supporting and supported organizations, customers, and stakeholders. Organizations plan for reconstitution prior to activation of their continuity plan and concurrently with continuity operations. However, reconstitution is implemented when the emergency, or threat of emergency, is over, and organizations initiate operations for resuming normal business operations.

See Annex N – Continuity Plan Operational Phases and Implementation

- 12. ROLES AND RESPONSIBILITIES:** Individuals at all levels of an organization maintain responsibility to ensure the continuation of essential functions during a continuity event. Assigned responsibilities are outlined in NSPD-51/HSPD-20 and the NCP/IP.
- 13. POINT OF CONTACT:** Should you have any questions or need additional assistance with the information contained in the FCD, please contact the Assistant Administrator, National Continuity Programs (NCP), FEMA, at 202-646-4145.
- 14. DISTRIBUTION:** This FCD is distributed to the heads of federal organizations, senior policy officials, emergency planners, and other interested parties.

ANNEX A. PROGRAM PLANS AND PROCEDURES

An organization implements an effective continuity program through its related plans and procedures, an effective continuity TT&E program, and an operational capability to support those plans and procedures. A critical part of developing a comprehensive continuity plan is the establishment of planning and procedural objectives and requirements and use of metrics to ensure that an essential function continues during a continuity activation, given the criticality and priority of the essential function.

Continuity planning is an effort to document and ensure the capability to continue organization essential functions during a wide range of potential emergencies. The objectives of continuity planning include:

1. Ensuring that an organization can perform its essential functions under all conditions;
2. Reducing the loss of life and minimizing property damage and loss;
3. Executing a successful order of succession with accompanying delegation of authorities in the event a disruption renders that organization's leadership and key personnel unavailable or incapable of assuming and performing their authorities and responsibilities of the respective office;
4. Reducing or mitigating disruptions to operations;
5. Ensuring that there are facilities from which organizations can perform essential functions;
6. Protecting personnel, facilities, equipment, records, and other assets critical to the performance of essential functions in the event of a disruption;
7. Achieving the organization's timely and orderly recovery and reconstitution from an emergency; and
8. Ensuring and validating continuity readiness through a dynamic and integrated continuity TT&E program and operational capability.

REQUIREMENTS FOR CONTINUITY PLANS AND PROCEDURES:

1. Organizations must develop and document a continuity plan and its supporting procedures so that, when implemented, the plan and procedures provide for the continued performance of an organization's essential functions under all circumstances and provide for integration with other Government and non-government organizations, as appropriate.
2. The Organization Head, such as the Secretary, Director, or Administrator, or a designee, must approve and sign the continuity plan, to include significant updates or addendums.
3. Organizations must annually review their continuity plan and update, if changes occur, and document the date of the review and the names of personnel conducting the review.
4. The continuity plan and procedures must:
 - a. Address the key elements of continuity: essential functions, orders of succession, delegations of authority, continuity facilities, continuity communications, essential records, human resources, TT&E, devolution, and reconstitution; and address the requirements associated with each element as found in this FCD;
 - b. Address the supporting elements of continuity: program plans and procedures, risk management, budgeting and acquisition, and operational phases and implementation; and address the requirements associated with each element as found in this FCD;

-
- c. Address the four phases of continuity: (1) readiness and preparedness, (2) activation, (3) continuity operations, and (4) reconstitution;
 - d. Provide a process for determining the organization's readiness posture and for decision-making regarding its corresponding actions to increase readiness postures. Federal Executive Branch HQ organizations must establish internal procedures for executing changes to the Continuity of Government Readiness Conditions (COGCON), as appropriate. Both HQ and non-HQ organizations must consider tribal, state, territorial, regional, or private sector continuity preparedness or activation directions in their internal procedures for executing changes to readiness levels;
 - e. Provide a process or methodology that ensures plan implementation, including a decision matrix for continuity plan activation with warning during duty and non-duty hours and without warning during duty and non-duty hours;
 - f. Establish and maintain appropriate relocation procedures and instructions for how ERG members will relocate to alternate sites;
 - g. Establish and maintain appropriate procedures and instructions on devolving functions to the DERG at a devolution site;
 - h. Detail the transition of responsibilities to the deployed ERG or DERG;
 - i. Provide a process for attaining operational capability at all continuity facilities within the minimal acceptable period for essential function disruption, but in all cases within 12 hours of plan activation for PMEFS and for MEFs and Essential Supporting Activities associated with the performance of PMEFS;
 - j. Provide a process or methodology ensuring that sustained operations can be maintained for up to 30 days or until normal operations resume. This includes planning for the challenges posed by extended events; and
 - k. Identify and establish procedures to ensure essential resources, facilities, and records are safeguarded, available, and accessible to support continuity operations. Essential resources should include ERG members, equipment, systems, infrastructures, supplies, and other assets required to perform an organization's essential functions.
5. Organizations must incorporate continuity requirements into their daily operations to ensure seamless and immediate continuation of essential function capabilities.
 6. Annually, all non-HQ organization entities, including subcomponent, regional and field offices, must submit the following documentation to its organization HQ, via appropriate reporting channels, to provide visibility on continuity efforts at all levels of the organization:
 - a. Certification by the Organization Head or a designee that the component/office maintains a continuity plan and the date of plan signature. Organizations may use regional or overarching continuity/devolution plans that integrate the continuity capabilities of multiple subordinate organizations; and
 - b. Certification by the Organization Head or a designee that the component/office participates in an annual exercise that incorporates the deliberate and preplanned movement of continuity personnel to an alternate site and the date of last exercise.
 7. Organization HQs must maintain a record of the date of continuity plan signature and last continuity exercise for the HQ and all components.
 8. Organization HQs must submit monthly Readiness Reporting System (RRS) reports.
-

ANNEX B. RISK MANAGEMENT

Risk management is 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.¹ Effective risk management practices and procedures will assist organizations in accomplishing continuity objectives.

An effective risk management program includes continuity of operations as part of its risk mitigation strategy. For this effort, the critical question will be: *How should I invest my limited resources across the four continuity pillars—leadership, staff, facilities and communications—to ensure that my organization satisfies its continuity requirements?*

When executing a risk management process for continuity operations, organizations consider a range of factors, such as the probabilities of events occurring, mission priorities, and impact assessments. Organizations should also consider cost, because informed decisions about acceptable and unacceptable levels of risk will ultimately drive the expenditure of resources (i.e., money, people, and time) to mitigate risk. Organizations can never fully mitigate risk, because no organization can afford to counter every threat to its mission. Successful continuity planning, then, demands an intelligent analysis and prioritization of where and when to focus resources and apply funding and other assets.

A continuity risk assessment includes an assessment of the likelihood of threats and hazards to normal operations and public safety, such as natural disasters, disruptions of communication, power, and other utilities, and acts of terrorism and war. It also includes an assessment of the consequences of any event that may occur in terms of continuity operations.

Risk management requires leadership to think beyond the internal effects of their organization's inability to perform essential functions. Organization leaders and staff at all levels need to also consider the interdependencies between and among organizations that share critical roles in the delivery of NEF capabilities. To the extent possible, organizations should partner with Tribal, State, Territorial, and local governments, as well as with owners and operators of private-sector CI and other relevant parties, to ensure continuity plans are coordinated between these entities and the Federal Executive Branch.

This annex provides an overview of risk management principles, the risk management process, and explains how to use the risk management process to promote continuity operation.

Risk Management Principles

A number of common principles should form the foundation for all risk management programs. These risk management principles offer broad guidance that organizations can uniquely tailor to their specific needs. These principles should include concepts such as *practicality*, which is based on the acknowledgement and acceptance of the limitations of the state of understanding regarding the various risks that organizations may face; *transparency*, which establishes that risk management information must be available and openly conveyed when appropriate; and

¹ Department of Homeland Security Risk Lexicon 2010.

adaptability, which relates to utilizing risk management practices in a manner that allows the process to remain dynamic and responsive to risk.

The Risk Management Process

The recommended risk management cycle to support continuity decision-making, which was introduced by DHS in 2009², is comprised of six analytical and management phases and entails:

1. Defining and framing the context of the decision and related goals and objectives to include an understanding of the kinds of risks associated with them;
2. Identifying the risks associated with the goals and objectives;
3. Analyzing and assessing the risks, with particular focus on the threats, vulnerabilities, and consequences;
4. Developing alternative strategies for managing the risks to essential functions and analyzing their costs and benefits;
5. Making a decision among alternatives, as well as communicating and implementing that decision; and
6. Monitoring the implemented alternatives to compare observed and expected effects, and influence subsequent risk management endeavors and decisions.

Risk communication underpins each phase of the risk management process. Risk communication is the exchange of information with the goal of improving risk understanding, affecting risk perception and/or equipping people or groups to act appropriately in response to an identified risk.



Figure 4: DHS Risk Management Process

The risk management process provides a useful framework for assessing the readiness and resiliency of an organization in performing its essential functions. The following sections describe the key elements that an organization should address in each of the phases of the risk management process.

1. Define the Context: The first step in the risk management process is to define the context of the decision that the risk management effort seeks to support. When scoping the requirements and constraints to be considered within a particular risk management process, the organization considers an array of variables:

1. The goals and objectives of the organization;
2. Its mission;
3. The scope and criticality of its essential functions; and
4. The decision timeframe for selecting continuity priorities.

² DHS Risk Management Fundamentals: Homeland Security Risk Management Doctrine, April 2011.

Organizations will individually tailor other variables:

1. Organizational risk management capabilities and resources;
2. The various stakeholders involved in continuity risk management;
3. The availability and quality of information on continuity risks; and
4. Any constraining factors.

By considering each of these elements systematically, decision makers and the analysts who support them are able to design an approach for identifying, assessing, and analyzing risks to an organization's essential functions and proposed risk management strategies that are commensurate with the organization's operating context.

2. Identify Potential Risk: Organizations should identify a preliminary list of risks to their essential functions using knowledge of the subject matter of the decision. Risks to continuity include exploring potential natural events, intentional man-made events, and non-intentional man-made events (also known as technological hazards) that could adversely affect the ability of the organization to perform essential functions. They also include other operational and institutional risks that could prevent an organization from performing its essential functions.

3. Analyze and Assess Risk: This phase of the cycle consists of gathering data, executing the continuity risk assessment methodology, and analyzing the results. To support decision making, analyzing and assessing risk is done via the following sub-steps.

Gathering data. Data are gathered to populate the assessment based on the requirements of the continuity risk assessment. While there are a number of potential sources for risk information, some of the most commonly used sources include historical records, elicitation of subject matter experts, and simulations. At this stage, initial data should be reviewed for potential errors.

Executing the methodology. Once the necessary data is gathered, the organization executes a risk assessment methodology. Many risk methodologies exist, so when choosing a risk assessment methodology, organizations should ensure to remain within their capabilities. The most important factor to consider in selecting a methodology is the decision the assessment must inform. Once a risk assessment methodology is chosen, the organization executes the methodology, re-checking the data for errors throughout the execution of the assessment, as the organization may not notice an error in an intermediate step. After the methodology has been fully executed, the organization should analyze its outputs.

Analyzing the results. Once the data are populated and the execution is complete, the results are then analyzed to identify relevant and interesting features for continuity of operations decision-making to promote better management of continuity risks. Results should be analyzed within organizations and, when appropriate, shared across the Federal Executive Branch.

4. Develop Alternatives: Developing alternatives is the process of creating viable options for managing risks in order to ensure decision makers are able to consider relevant, comparable, and scoped options that account for a comprehensive set of factors. The procedure for developing risk management strategies includes:

1. Considering opportunities for and constraints on risk treatment; and
2. Establishing a common framework to evaluate and compare alternatives.

When developing alternatives to manage risk, it is helpful to consider options in four categories:

Avoid: Risk avoidance refers to the process of removing risk by eliminating the situation or activity that presents the risk.

Control: Risk control refers to the process of identifying a risk and deciding on an option to reduce and control that risk to an acceptable level.

Accept: Risk acceptance refers to the concept that some risk cannot be eliminated, and that some risk may be worth assuming.

Transfer: Risk transfer refers to the process of transferring the risk to another stakeholder.

In considering alternative risk management treatments for promoting continuity, it is important to consider objectives, methods to achieve objectives, key constraints and the resources required to implement each treatment, as well as factors that would influence implementation and sustainability. Additionally, since risks often shift, it is important to revisit the alternatives development process, incorporate new information, and re-evaluate the options based on changed circumstances.

5. Decide Upon and Implement Risk Management Strategies: Decision makers need to consider the feasibility of implementing options to support continuity and how various alternatives affect and reduce risk. This includes the consideration of resources, capabilities, time to implement, political will, legal issues, the potential impact on stakeholders, and the potential for unintentionally transferring risk within the organization.

Once a decision has been made, the decision maker ensures that an appropriate management structure is in place to implement the decision. The decision maker should establish a program management approach, which will document the planning, organizing, and managing of resources necessary for the successful implementation of the risk management strategy.

6. Evaluation and Monitoring: After implementation of the strategies, the organization monitors whether the implemented risk management treatments achieve the desired goals and objectives, as well as whether the risks facing an organization are changing. This can be done via exercises, through real-world experience or through security vulnerability testing. A core element of the evaluation and monitoring phase involves using reporting on performance and results by developing concrete, realistic metrics.

It is critical that organizations assign responsibility for monitoring and tracking effectiveness of continuity efforts, and that evaluation methods are flexible and adaptable. Evaluating and monitoring implemented risk management strategies is similar to overall performance management of continuity activities. The results of the monitoring step should inform subsequent iterations of the risk management cycle.

The risk management cycle involves a series of steps that organizations can perform at different levels of detail with varying degrees of formality. The key to using this process to promote continuity of operations is completing each step in a way that provides accurate and adequate information to the decision maker so that he or she can make informed decisions about how best to manage risks to essential functions and ensure continuity.

REQUIREMENTS FOR RISK MANAGEMENT:

1. Organizations must apply a risk-based framework across all continuity efforts in order to identify and assess potential hazards, determine what levels of relative risk are acceptable, and prioritize and allocate resources and budgets to ensure continuity under all manner of incident conditions.
2. Organizations must conduct and document a risk assessment, to include a Business Impact Analysis, against all hazards at least every five years for all capabilities associated with the continuance of essential functions, to include all primary operating facilities, continuity facilities, personnel, systems, and records. These risk assessments provide reliable and comprehensive data to inform risk mitigation decisions that will allow organizations to protect assets, systems, networks, and functions while determining the likely causes and impacts of any disruption. The assessment must include:
 - a. Identification of potential, known risk, and the likelihood of its occurrence, which has direct impact on the ability of the organization to support the continuation of essential functions;
 - b. An assessment of the vulnerability of the organization and its essential functions to identified hazards;
 - c. An assessment of the impact of the failure of the identified essential functions caused by identified hazards;
 - d. Identification of appropriate mitigation and protective measures, to include measures necessary during a pandemic influenza;
 - e. A cost-benefit analysis of implementing risk mitigation, prevention, or control measures;
 - f. An operational plan to provide and implement selected mitigation, prevention, protection, or control measures, to include those necessary during a pandemic; and
3. Organizations must develop operational plans to provide and implement selected mitigation, prevention, protection, or control measures, to decrease the threat of and impact from identified risks, to include pandemic.
 - a. Organizations must conduct an analysis of the remaining risk based on implemented measures.

ANNEX C. BUDGETING AND ACQUISITION OF RESOURCES

It is critical for organizational resilience to identify the people, communications, facilities, infrastructure, and transportation requirements necessary for the successful implementation and management of an organization's continuity program. To support these programs, it is necessary to align and allocate the budgetary resources needed to acquire and then implement these requirements. Through the budgeting and planning process, an organization's leaders and staff will ensure the availability and resilience of critical continuity resources needed to continue performing the organization's essential functions before, during, and after a continuity activation.

The Director of the Office of Management and Budget (OMB) reviews all funding requests for continuity activities and evaluates organization performance in executing continuity budgets. Additional requirements for the Director of OMB are found in the NCPIP.

When developing continuity budgets or making acquisition decisions, an organization should consider:

1. Identifying the budgetary requirements for addressing organizational resilience and continuity interdependencies in the performance of internal and other organizations' essential functions;
2. Coordinating with the General Services Administration (GSA) to use pre-established acquisition, supply, storage, distribution and transportation mechanisms; and
3. Additional continuity factors such as probabilities of occurrence, mission priorities, and impact assessments, as part of the continuity risk management methodology.

Further, organizations may also consider cost, because informed decisions about acceptable and unacceptable levels of risk will ultimately drive the expenditure of resources (i.e., money, people, and time) to mitigate risk.

REQUIREMENTS FOR BUDGETING AND ACQUISITION:

1. Organizations must identify and provide continuity funding and specific budgetary requirements for all levels of their organizations, including subordinate components and regional and field offices, to establish and maintain the requirements for all elements of a viable and resilient continuity capability.
2. Organizations must develop a continuity Multi-Year Strategy and Program Management Plan (MYSPMP) that provides for the development, maintenance, and annual review of continuity capabilities, requiring an organization to consider:
 - a. Performance of essential functions;
 - b. Both short-term and long-term goals and objectives for plans and procedures;
 - c. Issues, concerns, and potential obstacles to implementing their program, as well as a strategy for addressing these, as appropriate;
 - d. Planning, training, and exercise activities, as well as milestones for accomplishing these activities;
 - e. ERG members, infrastructure, communications, transportation, and other resources needed to support the program;
 - f. Budgetary requirements to support the program;

- g. Risk management principles and primary operating facility and continuity facility risk assessments to ensure that appropriate operational readiness decisions are based on the probability of an attack or other incident and its consequences;
 - h. Geographic dispersion into the organization's normal daily operations, as appropriate;
 - i. The organization's security strategies that address personnel, physical, and information security to protect plans, personnel, facilities, and capabilities, to prevent adversaries from disrupting continuity plans and operations; and
 - j. A CAP that draws upon evaluations, after-action reports, and lessons learned from tests, training, and exercises and real world events.
- 3. Organizations must integrate continuity budgets with their MYSPMP and link the budgets directly to objectives and metrics set forth in that plan.
- 4. Organizations must identify provisions for the acquisition and procurement of necessary equipment, supplies, resources, and personnel that are not already in place at the continuity facilities on an emergency basis and needed to sustain operations for up to 30 days or until normal operations resume.
- 5. Organizations must budget for and acquire continuity capabilities in accordance with NSPD-51/HSPD-20 and National Communications System (NCS) Directive 3-10, as applicable.
- 6. Organizations must identify and integrate continuity requirements into existing and future contracts, as applicable, to ensure continuation of essential functions during crisis and sustainment for up to 30 days or until normal operations resume.
- 7. The Administrator of GSA, in collaboration with the Secretary of Homeland Security, shall identify GSA programs and acquisition vehicles capable of being used by all organizations for the purposes of planning for, detecting, responding to, and mitigating the effects of emergencies and disasters outlined herein.

ANNEX D. ESSENTIAL FUNCTIONS

The Federal Executive Branch recognizes that the entire spectrum of government functions may not be performed or needed in the immediate aftermath of an emergency. Indeed, in a crisis, resources may be scarce. Allocating resources based on sound planning helps to ensure that the delivery of essential functions will remain uninterrupted across a wide range of potential emergencies.

The identification and prioritization of essential functions is the foundation for continuity planning. Essential functions are 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 Essential Supporting Activities. FCD 2 provides detailed guidance to organizations to assist in the identification, prioritization, and resourcing of these essential functions. The immediacy of maintaining or recovering essential functions capability is driven by the results of Business Process Analyses (BPAs), as detailed in FCD 2.

Subsequently, the described risk management approach conducted via Business Impact Analyses (BIAs) requires an emphasis on the geographic dispersion, redundancy, and availability of leadership, staff, and infrastructure. Planners should assume that they will have no warning of the threats faced in today's world. Threats might come from known or unknown sources and do not necessarily emanate from a single, fixed, and understood actor. Threats require planners to consider different approaches to plan for, mitigate, and respond.

REQUIREMENTS FOR ESSENTIAL FUNCTIONS:

1. Organizations must identify and prioritize their essential functions, using the methodology outlined in FCD 2, and document them in its continuity plan. These essential functions serve as the framework for the continuity plan and organizations should account for all continuity capabilities required for the performance essential functions.
2. Organizations must review their government functions to determine those directed by applicable laws, presidential directives, executive orders, and other directives.
3. Organizations must conduct a BPA to determine the essential functions that they must perform under all circumstances either uninterrupted, with minimal interruption, or requiring immediate execution in an emergency.
 - a. The BPA must identify and map the functional processes, workflows, activities, resources, personnel expertise, supplies, equipment, infrastructures, systems, data, and facilities inherent to the execution of each identified essential function.
 - b. The organization head or designee must validate and approve the identified essential functions and BPA.
4. Organizations must conduct a business-process flow map to identify how each essential function is performed and executed.
5. Organizations must determine the PMEFs that need to be continued uninterrupted or resumed within 12 hours, regardless of circumstance.

6. Organizations must identify internal and external interdependencies that are part of and/or influence each essential function business process.
7. Organizations must identify those essential functions that provide interdependent support to an essential function performed by another organization, including when and where the vital support would be provided.
8. Organizations must annually review their essential functions and BPAs and document the date of the review and names of personnel conducting the review. Organizations must incorporate any identified changes generated by new organization programs or functions or by organizational changes to existing programs or functions.

ANNEX E. ORDERS OF SUCCESSION

Leadership is responsible for establishing, promulgating, and maintaining orders of succession to key positions. It is critical to have a clear line of succession established in the event an organization's leadership becomes debilitated or incapable of performing its legal and authorized duties, roles, and responsibilities. The designation as a successor enables that individual serve in the same position as a principal in the event of that principal's death, incapacity, or resignation. Orders of succession are prepared to provide clarity of leadership in the event that individuals serving in senior leadership, key decision-making, or management roles are unavailable.

Orders of succession are a formal, sequential listing of organization positions (rather than specific names of individuals) that identify who is authorized to assume a particular leadership or management role under specific circumstances. Orders of succession enable an orderly and predefined transition of leadership within the organization. Orders of succession are an essential part of an organization's continuity plans and should reach to a sufficient depth and have sufficient breadth to ensure the organization can perform its essential functions while remaining a viable part of the Federal Government during the course of any emergency. Geographical dispersion, including use of regional, field, or satellite leadership in the standard organization line of succession, is encouraged and ensures roles and responsibilities can transfer in all contingencies.

In some cases, orders of succession are prescribed by statute. In other cases, an organization may have the latitude to develop orders of succession for particular positions to ensure critical decisions can be made during temporary absences of senior personnel.

REQUIREMENTS FOR ORDERS OF SUCCESSION:

1. Organizations must establish and document orders of succession in advance and in accordance with applicable laws to ensure there is an orderly and predefined transition of leadership during any emergency.
2. Organizations must establish an order of succession for the position of organization head to ensure a designated official is available to serve as acting head of the organization until that official is appointed by the President or other appropriate authority, replaced by the permanently appointed official, or otherwise relieved.
3. Organizations must establish orders of succession for other key organization leadership positions, including, but not limited to, administrators, regional or field directors, and key managers.
4. Within each order of succession, organizations must include at least three positions permitted to succeed to the identified leadership position.
5. Organizations must describe orders of succession by positions or titles, rather than by the names of the individuals holding those offices.
6. Heads of Category I and II HQ organizations, as identified in NSPD-51/HSPD-20, must include at least one individual in their order of succession who is geographically dispersed from the organization head and other individuals within the order of succession. All organizations should include an individual who is geographically dispersed in all HQ and non-HQ orders of succession, where feasible.

7. Organizations at all levels must coordinate the development and revision of orders of succession with their general counsel or chief counsel to ensure legal sufficiency.
8. Organizations must include orders of succession in the essential records and ensure they are available at all continuity facilities.
9. Organizations must revise orders of succession, as necessary, and distribute the revisions promptly as changes occur to higher organization authorities, potential successors, affected staff, and others, as appropriate.

ANNEX F. DELEGATIONS OF AUTHORITY

To ensure a rapid response to any emergency and to minimize disruptions that require implementation of continuity plans, organizations pre-delegate the authority to make policy determinations and decisions, at the HQ, regional, field, satellite, and other offices, as appropriate. Delegations of authority ensure the orderly and predefined transition of leadership responsibilities within an organization during a continuity activation and are closely tied to succession. A 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, including limitations, conditions, and restrictions, that an individual is deemed by the organization as qualified to perform.

To the extent possible, organizations should identify the individuals to whom authorities are delegated by position title and not by name. At minimum, a delegation of authority should exist for the individuals listed in the orders of succession. Delegations of authorities are frequently tied to specific positions, but since many delegations require specific training, qualifications, and certification, organizations must associate some delegations of authority with a specific individual.

Generally, predetermined delegations of authority will take effect when normal channels of direction are disrupted and will terminate when these channels are reestablished. Delegation of authority is an essential part of an organization's continuity plans and should reach to a sufficient depth and have sufficient breadth to ensure the organization can perform its essential functions while remaining a viable part of the Federal Government during the course of any emergency.

REQUIREMENTS FOR DELEGATIONS OF AUTHORITY:

1. In accordance with applicable laws, organizations must establish and document in advance the legal authority for the position of Organization Head and other key supporting positions to make key policy decisions during a continuity situation, including:
 - a. Outlining explicitly in a statement the authority, including any exceptions to that authority, of an official so designated to exercise organization direction;
 - b. Delineating the limits of authority and accountability;
 - c. Establishing the rules and procedures designated officials must follow when facing the issues of succession to office;
 - d. Outlining the authority of officials to re-delegate functions and activities, as appropriate;
 - e. Defining the circumstances under which delegation of authorities would take effect and would be terminated; and
 - f. Incorporating the conditions under which delegations will 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. Organizations must inform those officials listed within the delegations of authority who might be expected to assume authorities in a continuity activation.
3. Organizations must include delegations of authority as an essential record and ensure they are available at all continuity facilities.
4. Organizations at all levels must coordinate the development and revision of delegations of authority with their general counsel or chief counsel to ensure legal sufficiency.

ANNEX G. CONTINUITY FACILITIES

The use of continuity facilities, alternate usages of existing facilities, and telework options enhances the resiliency and continuity capability of organizations. When identifying and preparing continuity facilities, organizations should maximize use of existing local or field infrastructures, including consideration for other supporting options such as telework, mobile work, and joint or shared facilities. Additionally, it is financially prudent to structure and configure continuity facilities such that organizations can replace or augment daily activities with those required during an emergency. Organizations must establish and select continuity facilities using an accounting of the risks associated with natural disasters, power outages, information technology issues, and other threats. Organizations should select and construct facilities 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.

The term “continuity facilities” is comprehensive, referring to both continuity and devolution sites where essential functions are continued or resumed during a continuity event. “Alternate sites” are locations, other than the primary facility, used to carry out essential functions by relocating ERG members following activation of the continuity plan. “Devolution sites” are locations used to carry out essential functions by devolving the essential functions to a geographically-separated facility and staff (the DERG) following activation of the devolution plan. These sites refer to not only other facilities and locations, but also work arrangements such as telework and mobile work concepts.

A continuity facility may be classified as one of the following three types:

1. Hot site: A continuity facility that already has in place the computer, telecommunications, other information technology, infrastructure, and personnel required to recover essential functions.
2. Warm site: A continuity facility that is equipped with some computer, telecommunications, other information technology, and environmental infrastructure, which is capable of providing backup after additional personnel, equipment, supplies, software, or customization are provided.
3. Cold site: A facility that is not manned on a day-to-day basis by personnel from primary operating facility. Organizations may be required to pre-install telecommunication equipment and IT infrastructure upon selection/purchase and deploy designated IT essential personnel to the facility to activate equipment/systems before it can be used.

Organizations may make use of existing organization or other space for continuity facilities:

1. Remote/offsite training facilities: These facilities may include an organization training facility located near the organization’s normal operating facility, but far enough away to afford some geographical dispersion.
2. Regional or field offices: Some organizations have a regional office or a field office that they can use as a continuity facility.
3. Remote HQ operations: Some organization HQ operations are so extensive that their operations and the facilities required to support them extend beyond the geographic expanse of the organization HQ host city, and necessitate an additional HQ location(s) elsewhere. One of these locations could serve as continuity facility.

4. Memorandum of Agreement (MOA)/Memorandum of Understanding (MOU) for co-location with another organization: One organization may relocate to another organization's facilities. The organization that is relocating could occupy available space in the receiving organization's HQ or training facilities, field offices, or other spaces.
5. Space procured and maintained by GSA: An organization may request GSA to acquire, equip and sustain both privately and/or federally-owned and leased space to accommodate that organization's need for continuity facilities.
6. Space procured and maintained by another organization: Some organizations, other than GSA, offer space procurement services that organizations can use for continuity facilities.
7. Participation in a joint-use continuity facility: Several organizations may pool their resources to acquire space they can use jointly as a continuity facility. With this option, organizations will ensure that shared facilities are not overcommitted during a continuity activation. An organization may co-locate with another organization at a continuity facility, but each organization should have individually designated space and other resources at that location to meet its own needs.
8. Alternate use of existing facilities: In certain types of continuity activations, organizations may use a combination of facilities and strategies, such as social distancing, to support continuity operations.
9. Telework: The official definition of telework, as found in the Telework Enhancement Act of 2010, is "a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work." Many organizations have programs that allow employees to telework. This capability is leveraged to allow ERG members to fulfill their essential functions at an approved alternative worksite (such as at home or a telework center).
10. Mobile work: Mobile work is characterized by travel to conduct work in customer or other worksites as opposed to a single authorized alternative worksite, such as work performed while commuting, traveling between worksites, or on temporary duty. This capability includes the use of mobile drive-away kits (such as laptop computers, cell phones, and satellite communications equipment), which can be readily transported to a remote location.

REQUIREMENTS FOR CONTINUITY FACILITIES:

1. At a minimum, organizations must identify, prepare, and maintain continuity facilities, including an alternate site for the relocation of their ERG and a devolution site for the devolution of essential functions to the DERG. This capability can encompass separate facilities; alternate usages of existing facilities; and, as appropriate, work arrangements, including telework and mobile work. It is recommended that organizations coordinate with GSA for assistance in identifying physical relocation sites.
2. Organizations must review continuity facilities for their suitability and functionality at least annually, to ensure that the facilities meet their continuity requirements, and document the date of the review and names of personnel conducting the review.
3. Organizations must choose continuity facilities located in areas where the potential disruption of the organization's ability to initiate and sustain operations is minimized, based upon their risk assessments.

4. Continuity facilities must have sufficient distance, based upon risk assessments and as judged by the organization, from the primary operating facility, threatened area, and other facilities or locations that are potential sources of disruptions or threats.
5. Organizations must have all critical supplies and equipment pre-positioned or maintain detailed site preparation and activation plans in order to achieve full operational capability within 12 hours of notification.
6. After selecting appropriate facilities for continuity operations, organizations must ensure the continued availability of facility space and services by coordinating with site facility managers and property owners, if applicable.
7. If the continuity facilities are neither owned nor leased by the organization, organizations must prepare and sign a MOA/MOU with the owner or occupant of the facility and review the MOA/MOU annually, documenting the review with the date of review and names of personnel conducting the review. At a minimum, MOAs/MOUs must specify:
 - a. The required notification time for owner/occupant of the facility to have it configured and available for occupancy as a continuity facility;
 - b. Space and services to be provided at the facility; and
 - c. Sole use of allocated space by the organization during the period of occupancy.
8. Organizations must establish and maintain procedures for the orientation, in-processing, and reception of ERG and DERG personnel and for conducting operations and administration at all continuity facilities.
9. All U.S. Government organizations and their associated entities (including HQ, regional, and field offices), must report the locations of their alternate sites (not devolution sites) for entry in a classified central database, per NCPIP mandate. Organizations can meet compliance via completion and submission of the Standard Form (SF)-336, "GSA Alternate Facility Reporting Form" available via classified systems at <https://gsapergamum.gold.ic.gov>. Organizations without access to classified systems can access this form via unclassified means at gsa.gov/forms and submit via classified fax at 202-501-1068. Organizations are required to annually review and re-submit their SF-336. Organizations may contact GSA's Office of Emergency Response and Recovery at eoc@gsa.gov and/or 202-501-0012 for further instructions.
10. Identified alternate and devolution sites must ensure the following, by either ensuring the capability exists at the facility prior to activation or by ensuring availability within 12 hours for PMEFs and within the acceptable recovery time determined for other essential functions:
 - a. Replication of essential capabilities by providing systems and configurations that are used in daily activities;
 - b. Interoperable communications, including the means for secure communications if appropriate, with all identified essential internal and external organizations, as well as with customers and the public;
 - c. Computer equipment, software, and other automated data processing equipment necessary to carry out essential functions and information systems are up-to-date with the latest software and system updates;
 - d. Capabilities to access and use essential records necessary to facilitate the performance of essential functions;

- e. The capability to perform essential functions as soon as possible after continuity activation with minimal disruption of operations, the ability to maintain this capability for up to 30 days or until normal operations resume, and the capability to perform these essential functions under all threat conditions;
- f. Reliable logistical support, services, and infrastructure systems;
- g. Consideration of the availability of essential support resources such as food, water, fuel, medical facilities, and municipal services, such as fire and police, to ensure the health, safety, and security of ERG/DERG members;
- h. Emergency/back-up power capability, so that essential functions and operations can continue in the event the primary source of power is disrupted;
- i. Housing to support the ERG/DERG at or near the continuity facilities, such as billeting within the facility, other locations, including motels, or at ERG/DERG members' homes if within commuting distance to the continuity facility;
- j. A defined transportation support plan that details ERG/DERG transportation to, from, and on the site; and
- k. 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 organization policy.

Telework

All organizations must incorporate telework into their continuity plan and procedures by:

1. Assessing the organization's essential functions to identify which functions the organization must conduct onsite and which functions the organization can conduct via telework, including evaluating the use of telework for supporting extended continuity operations and use by non-ERG personnel.
 - a. For those essential functions that employees must conduct onsite, organizations must classify jobs by exposure risk level to pandemic influenza. Organizations must notify these employees that they are expected to work onsite during an influenza pandemic.
2. Establishing and maintaining plans and procedures to use telework as a primary or back-up continuity strategy for those essential functions and supporting tasks that are telework authorized, based upon the assessment.
3. Establishing a policy under which eligible employees, both ERG and non-ERG personnel, are authorized to telework during a continuity event.
4. Notifying all employees of their eligibility to telework during a continuity activation.
5. Ensuring that each eligible employee is authorized to telework during a continuity activation by successfully completing an interactive telework training program prior to entering into and signing a written telework agreement with his/her supervisor.
6. Coordinating with the organization's designated Telework Managing Officer when developing and integrating the organization's continuity plan.

Organizations using telework as a primary or back-up continuity strategy must:

1. Adhere to policy and guidance governing the use of telework.³
2. Provide protection of information and information systems used during telework activities according to government standards.⁴
3. Coordinate with the organization's Chief Information Officer to identify equipment and technical support requirements.
4. Provide access to essential records and databases and the robust communications necessary to sustain an organization's essential functions at the telework site locations.
5. Ensure continuance of a viable continuity capability in the event that telework is not a viable option (i.e. significant electrical and/or telecommunications infrastructure degradation).

³The Office of Personnel Management in the areas of pay and leave, agency closure, performance management, official worksite, recruitment and retention, and accommodations for employees with disabilities; FEMA in the areas of continuation of operations and long-term emergencies; the General Services Administration in the areas of telework centers, travel, technology, equipment, and dependent care; and the National Archives and Records Administration in the areas of efficient and effective records management and the preservation of records, including Presidential and Vice-Presidential records.

⁴ Federal Information Security Management Act of 2002.

ANNEX H. CONTINUITY COMMUNICATIONS

The success of continuity programs is dependent on the availability of robust and effective communications to provide federal intra- and interagency connectivity. An organization's ability to execute its essential functions at its primary operating facility and continuity facilities, as well as the ability of the organization's senior leadership to collaborate, develop policy and recommendations, and act under all-hazards conditions, depends upon the availability of effective communications systems. These systems support full connectivity, under all conditions, among key government leadership, internal elements, other organizations, critical customers, and the public. The Office of the Manager of the NCS is responsible for coordinating the publication of a compendium of all communications capabilities required in NCS Directive 3-10, dated 2011.

In support of continuity communications, the Continuity Communications Architecture (CCA), is an integrated, comprehensive, interoperable information architecture, developed utilizing the OMB-sanctioned Federal Enterprise Architecture Framework. The CCA describes the data, systems, applications, technical standards, and underlying infrastructure required to ensure that Federal Executive Branch organizations can execute their PMEfs in support of NEFs and continuity requirements under all circumstances.

REQUIREMENTS FOR CONTINUITY COMMUNICATIONS: All organizations must consider and address telecommunication services availability needs at primary and continuity facilities, in compliance with Office of Management and Budget Memorandum M-05-16 and NCS Handbook 3-10-1. In accordance with these documents and NCS Directive 3-10, NCS Directive 3-1, and Intelligence Community Standard Number 500-19:

1. Organizations that directly support NEFs must possess, operate, and maintain, or have dedicated access to, communications capabilities at both their primary operating facility and continuity facility locations, as well as mobile, in-transit communications capabilities (secure cell and secure satellite phones for Category I, II, and III organizations) for their senior leadership, commensurate with their category and communications capabilities, to ensure the continuation of those organizations' essential functions across the full spectrum of hazards, threats, and emergencies, including catastrophic attacks or disasters. Secure and non-secure communications requirements should be incorporated, as applicable.
2. Organizations that do not directly support NEFs must possess, operate, and maintain, or have dedicated access to, communications capabilities at both their primary operating facility and continuity facility locations, as well as mobile in-transit communications capabilities for their senior leadership capabilities, as required, to ensure the continuation of those organizations' essential functions. Secure and non-secure communications requirements should be incorporated, as applicable.
3. Category I and select Category II organizations, as identified in NSPD-51/HSPD-20, must coordinate with the Secretary of Homeland Security and the Secretary of Defense to obtain and operate secure and integrated COG communications. Organizations must document classified information in classified annexes of relevant continuity and communications plans.

4. Organizations who share a continuity facility with another organization must have a signed agreement with that organization to ensure each has adequate access to communications resources.
5. Organizations must possess interoperable and available communications capabilities in sufficient quantity and mode/media that are commensurate with that organization's responsibilities during conditions of an emergency.
6. Organizations must possess communications capabilities that support the organization's senior leadership while they are in transit to continuity facilities.
7. Organizations must ensure that the communications capabilities required by this Directive are maintained, are operational as soon as possible following a continuity activation, and in all cases within 12 hours of continuity activation, and are readily available for a period of sustained usage for up to 30 days or until normal operations can be reestablished. Organizations must plan accordingly for essential functions that require uninterrupted communications and IT support, if applicable.
8. The Office of the Manager of the NCS coordinates mandatory testing for NCS Directive 3-10. Organizations must report on continuity communications capability on a quarterly basis to an official designated by the Chief of Staff to the President or the Manager of the NCS.
9. Organizations with Top Secret/Sensitive Compartmented Information systems that are interoperable with the Joint Worldwide Intelligence Communications System at their continuity facility must ensure universal and remote access in compliance with Intelligence Community Standard Number 500-19.
10. Organizations must issue all ERG members Government Emergency Telecommunications Service (GETS) cards and pre-position GETS cards for emergency use at all primary and continuity facilities in the quantity equal to 50% of the total number of ERG personnel who are assigned to use the particular facility.
11. The government-issued cellular telephones for all ERG members must be Wireless Priority Service (WPS)-capable and have WPS activated.
12. All primary and continuity facility circuits supporting continuity communications must be included in the Telecommunications Service Priority program.
13. Organizations must annually review their continuity communications to ensure they are fully capable of supporting essential functions and document the date of review and the names of personnel conducting the review.
14. The Administrator of GSA, in collaboration with the Secretary of Homeland Security and NCS, shall identify GSA programs and acquisition vehicles to allow for the consolidated acquisition of interoperable communications equipment bridging all levels of classification.

Organizations may request an exemption from one or more of these minimum communications requirements by submitting a request by letter through the Office of the Manager of the NCS, for decision by the Director of the Office of Science and Technology Policy, in coordination with the National Continuity Coordinator. The request must identify the specific requirement and provide a detailed justification for the requested exception. A lack of funds is not considered a valid justification for an exemption.

ANNEX I. ESSENTIAL RECORDS MANAGEMENT

The identification, protection, and ready availability of essential records, databases, and hardcopy documents needed to support essential functions under the full spectrum of all-hazards emergencies are critical elements of a successful continuity plan and program. Organizations should strongly consider multiple redundant media for storing their essential records.⁵

In this document, “essential records” refers to information systems technology, applications, and infrastructure, electronic and hardcopy documents, references, and records needed to support the continued performance of essential functions during a continuity activation. 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 those records to the appropriate personnel.

Categories of essential records include the following:

1. **Emergency Operating Records:** These include records and databases essential to the continued functioning or the reconstitution of an organization during and after a continuity activation. Examples of these 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 ERG with the guidance they need to conduct operations during a continuity situation and to resume normal operations at the conclusion of that situation.
2. **Rights and Interests Records:** These include records 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. These records include those with such value that their loss would significantly impair the execution of essential organization 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. Any Rights and Interests Records considered critical for continued performance of essential functions should be included in the Emergency Operating Records and maintained at the appropriate continuity facility.

⁵ Additional information on records management can be found in: 36 Code of Federal Regulations, Part 1236, *Electronic Records Management*, November 2009; 44 Code of Federal Regulations, Part 3541, *Federal Information Security Act of 2002*; National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010; National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Systems and Organizations*, August 2009.

REQUIREMENTS 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;
 - b. Identify and protect those records necessary to the organization's continuing essential functions and resumption of normal operations;
 - c. Identify and protect those records needed to protect the legal and financial rights of the Government and citizens; and
 - d. Include appropriate policies, authorities, procedures and the written designation of an essential records manager.
 2. Organizations must incorporate their essential records program into their overall continuity plans.
 3. Organizations must develop procedures to ensure that as soon as possible after activation of continuity plans, but in all cases within 12 hours of an activation, ERG/DERG at the continuity facilities have access to the appropriate media for accessing essential records.
 4. Organizations must maintain a complete inventory of essential records, along with the locations of and instructions on accessing those records. This inventory must be maintained at a back-up/off-site location to ensure continuity if the primary operating facility is damaged or unavailable. Organizations should consider maintaining these inventories at a number of different sites to support continuity operations.
 5. Organizations must conduct an essential records and database risk assessment to:
 - a. Identify the risks involved if essential records are retained in their current locations and media, and the difficulty of reconstituting the records if destroyed;
 - b. Identify off-site storage locations and requirements;
 - c. Determine if alternative storage media is available; and
 - d. Determine requirements to duplicate records and provide alternate storage locations to provide readily available essential records under all conditions.
 6. Organizations must make appropriate protections for essential records, to include dispersing those records to other organization locations or storing those records offsite. When determining and selecting protection methods, it is important to take into account the special protections needed by different kinds of storage media.
 7. Organizations must develop and maintain an essential records plan packet and include a copy of the packet at the continuity facilities. An essential records plan packet is an electronic or hard copy compilation of key information, instructions, and supporting documentation needed to access essential records in an emergency situation. Organizations must annually review this packet and document the date of the review and the names of personnel. The packet must include:
 - a. A hard or soft copy of ERG members with up-to-date telephone numbers;
 - b. An essential records inventory with the precise locations of essential records;
 - c. Necessary keys or access codes;
 - d. Continuity facility locations;
 - e. Access requirements and lists of sources of equipment necessary to access the records (this may include hardware and software, microfilm readers, Internet access, and/or dedicated telephone lines);
 - f. Lists of records of recovery experts and vendors; and
 - g. A copy of the organization's continuity plans.
-

8. At a minimum, organizations must annually review, rotate, or cycle essential records so that the latest versions are available.
9. Organizations must annually review their essential records program to address new security issues, identify problem areas, update information, and incorporate any additional essential records generated by new organization programs or functions or by organizational changes to existing programs or functions. Organizations must document the date of the review and the names of personnel conducting the review.
10. Organizations must develop instructions on moving essential records (those that have not been prepositioned) from the primary operating facility to the alternate site and include these instructions in its continuity plan.

ANNEX J. HUMAN RESOURCES

Staff is vital to the continuity capability of all organizations. Continuity Coordinators at each executive branch organizations are senior accountable officials at the Assistant Secretary (or equivalent) level responsible to work with their Organization Head to ensure effectiveness and survivability of the organization's continuity capability. Meanwhile, Continuity Managers manage the day-to-day continuity programs.

During a continuity activation, organizations will activate ERG members to perform their assigned duties. The ERG is comprised of individuals who are assigned responsibility to relocate to an alternate site, as required, to perform organization essential functions or other tasks related to continuity operations. Personnel stationed at the devolution site who are identified to conduct essential functions during activation of devolution plans are classified as the DERG. Organizations should consider rotating on-call requirements for ERG and DERG members, where possible, or permitting primary and alternate ERG and DERG personnel to trade coverage times to provide relief from remaining in a constant state of readiness. While the law does not provide compensation for being in an "on-call" status, organizations should consider awards to recognize and honor exceptional employee contributions to continuity. Organizations should review position descriptions of any personnel who spend a substantial amount of time on a regular and continuing basis on continuity activities in order to determine if such duties are documented in the official position description of record and to ensure that the addition of such duties does not impact the position's title, series, and/or grade.

In addition to supporting the human resources needs of ERG and DERG members, organizations are also responsible for supporting employees who are not designated as ERG personnel (referred to as non-ERG members), but who may also be affected by a continuity activation. Procedures and expectations for these employees should be addressed in continuity and emergency plans, such as the OEP, which includes evacuation and shelter-in-place planning. Further, staff accountability is a critical capability for all organizations. Organizations must have a means and processes in place for employees to contact their organization in a timely and routine manner.

The Importance of Telework for Emergency Planning

The Telework Enhancement Act of 2010 states that "each executive agency shall incorporate telework into the continuity of operations plans for that agency." Incorporating telework into continuity plans means that these plans identify ways that an organization's personnel perform the duties and responsibilities necessary to continue the organization's essential functions during any type of threat or emergency from an approved worksite other than the location from which the employee would otherwise work. Requirements for organizations as it relates to incorporating telework into continuity plans are found in Annex G.

For more information on telework, refer to www.telework.gov. For more information on "Requirements for Emergency Employees and Telework", refer to the U.S. Office of Personnel Management (OPM) *Washington, DC, Area Dismissal and Closure Procedures* at www.opm.gov.

Emergency Employees

In addition to identifying ERG and DERG personnel who are responsible for the continuation of essential functions during a continuity activation, organizations are also responsible for identifying other categories of employees. While furlough, dismissal, and closure situations do not inherently lead to the activation of an organization's continuity plan, organizations must plan for such a scenario.

“Emergency employees” are critical to organization operations (including security and infrastructure) in dismissal and closure situations and who will be expected to work. Organization Heads are responsible for identifying “emergency employees” based on the organization's unique mission requirements and/or circumstances and can find additional references and information at www.opm.gov⁶. Further, organizations may need to designate those personnel who are allowed to work during a shutdown furlough or money-saving furlough (referred to as exempt employees). If a continuity activation occurs during a period of time during which employees are affected by a shutdown furlough or money-saving furlough, each organization will have to determine whether each individual employee may or may not participate in the continuity operations under applicable law and based on budget conditions, funding sources, and mission priorities. Employees participating in continuity events are not automatically excepted or exempt from a furlough.

REQUIREMENTS FOR HUMAN RESOURCES:

1. Organizations must develop and implement processes to identify, document, and prepare ERG members who are capable of relocating to alternate sites or teleworking and DERG members at the devolution site to support the continuation of the performance of essential functions.
 - a. Organizations must clearly define the expectations, roles and responsibilities of ERG and DERG members during a continuity activation.
 - b. Organizations must establish and maintain appropriate point-of-contact rosters of trained ERG and DERG members who have the ability to perform essential functions. Organizations must update these rosters periodically and include, at a minimum, names, home, work, and cell telephone numbers.
 - c. Organizations must ensure that ERG and DERG members are officially informed of and accept their roles and responsibilities by providing documentation these individuals.
 - d. Organizations must identify replacement personnel and augmentees, as necessary.
 - e. If bargaining unit employees are included as ERG or DERG members, organizations must ensure that all applicable collective bargaining obligations are satisfied.
2. Organizations must provide guidance to ERG members on individual preparedness measures they should take to ensure response to a continuity activation.

⁶ OPM Guide to Telework in the Federal Government; OPM Washington, DC, Area Dismissal and Closure Procedures; OPM Handbook on Pay and Leave Benefits for Federal Employees Affected by Severe Weather Conditions or Other Emergency Situations; OPM Human Resources Flexibilities and Authorities in the Federal Government.

3. Organizations must recommend the content and maintenance of drive-away kits for ERG members.
4. Organizations must provide guidance to all staff in preparing, planning and staying informed during an emergency, including developing Family Emergency Plans.
5. Organizations must implement a process to communicate the organization's operating status to all staff.
6. Organizations must implement a process to contact and account for all staff, including contractors, in the event of an emergency. All staff, including contractors, must know their responsibilities to report their accountability.
7. Organizations must establish procedures and provide the ability to communicate with and coordinate activities with all personnel; continuity facilities and support teams; organizations with which the affected organization interacts; customers; and stakeholders before, during, and after a continuity event, including alert and notification.
8. Organizations must work with their labor unions in developing and bargaining over such procedures where bargaining unit employees are impacted.
9. Organizations must communicate how, and the extent to which, employees are expected to remain in contact with their organizations during any closure situation.
10. Organizations must establish and maintain procedures to provide guidance to non-ERG personnel.
11. Organizations must facilitate dialogue among the Director of Human Resources, Telework Managing Officer, and Continuity Manager when developing their continuity plans.
12. Organizations must implement a process to communicate their human resources guidance for emergencies, such as pay, leave, staffing, and other human resources flexibilities, to all staff.
13. Within their continuity plans and procedures, organizations must include or reference provisions and procedures for assisting all staff, especially those who are disaster survivors, with special human resources concerns following a catastrophic disaster.
14. An organization's continuity program, plans, and procedures must incorporate or reference existing organization-specific guidance and policy for human resource management, such as guidance on pay, leave, work scheduling, benefits, telework, hiring, authorities, and flexibilities.

ANNEX K. TEST, TRAINING, AND EXERCISE PROGRAM

An effective TT&E program is necessary to assist organizations to prepare and validate their organization's capabilities and program and to the Federal Executive Branch's ability to perform essential functions during any emergency.

The testing, training, and exercising of continuity capabilities is essential to demonstrating, assessing, and improving an organization's ability to execute its continuity program, plans, and procedures. The testing of an organization's ability to demonstrate continuity capabilities in the performance of essential functions enables leadership to establish clear goals for the organization. This periodic testing also ensures that resources and procedures are kept in a constant state of readiness. Training familiarizes continuity personnel with their roles and responsibilities in support of the performance of an organization's essential functions during a continuity event. Exercises prepare ERG and DERG members to respond to all emergencies and disasters and ensure performance of the organization's essential functions. These include interdependencies both internal and external to the organization.

An organization's continuity exercise program focuses primarily on evaluating capabilities or an element of a capability, such as a plan or policy, in a simulated situation. The Homeland Security Exercise and Evaluation Program (HSEEP) is a capabilities- and performance-based exercise plan that provides a standardized policy, methodology, and language for designing, developing, conducting, and evaluating all exercises. The HSEEP is a pillar of the National Exercise Program framework. Organizations should refer to the HSEEP for additional exercise and evaluation guidance. Annual requirements are defined as occurring during the federal fiscal year, not every 365 days.

REQUIREMENTS FOR TT&E:

1. Organizations must develop and maintain a continuity TT&E program for conducting and documenting TT&E activities that identifies the components, processes, and requirements for the training and preparedness of personnel needed to support the continuation of the performance of essential functions.
2. As part of its TT&E program, the organization must document all conducted TT&E events, including documenting the date of the event, those participating in the event, and the results of the event.
3. The organization TT&E program must utilize an all-hazards approach to demonstrate the viability of their continuity plans and programs.
4. Continuity personnel must demonstrate their understanding of and ability to perform their assigned roles and responsibilities through participation in their organization's continuity TT&E program.

Testing

An organization's testing program must include and document:

5. Annual testing of alert, notification, and activation procedures for continuity and devolution personnel and quarterly testing of such procedures for personnel at the organization's HQ.

6. Annual testing of recovery strategies for essential records (both classified and unclassified), critical information systems (both classified and unclassified), services, and data.
7. Annual testing of the capabilities for protecting essential records and information systems (both classified and unclassified) and for providing access to them from the continuity facilities.
8. Annual testing of primary and backup infrastructure systems and services, such as power, water, and fuel, at continuity facilities.
9. Annual testing and exercising of required physical security capabilities at continuity facilities.
10. Quarterly testing of the internal and external interoperability and viability of communications equipment and systems.
11. Annual testing of the capabilities required to perform an organization's essential functions, as identified in the BPA.
12. Annual testing of telework capabilities, to include IT infrastructure, required to support telework options during a continuity event.
13. Annual testing of internal and external interdependencies identified in the organization's continuity plan, with respect to performance of an organization's and other organizations' essential functions.

Training

An organization's training program must include and document:

14. Annual continuity awareness briefings or other means of orientation for the entire workforce.
15. Annual training on the roles and responsibilities for personnel, including host or contractor personnel, who are assigned to activate, support, and sustain continuity and devolution operations.
 - a. Annual briefings for ERG and DERG members on organization continuity and devolution plans that involve using, or relocating to, continuity facilities, existing facilities, or other work arrangements, such as telework.
 - b. Annual training for ERG and DERG members on all reconstitution plans and procedures to resume normal organization operations at the original primary operating facility or replacement primary operating facility.
 - c. Annual training for ERG and DERG members on the activation of continuity plans, including unannounced relocation to alternate sites, to include telework options, and devolution of operations to devolution sites.
 - d. Annual training for ERG and DERG members on the capabilities of communications and IT systems to be used during a continuity or devolution event.
 - e. Annual training for ERG and DERG members regarding identification, protection, and ready 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 essential functions during a continuity or devolution activation.
 - f. Annual training for ERG and DERG members on an organization's devolution option for continuity, to address how each organization will identify and conduct

its essential functions during an increased threat situation or in the aftermath of a catastrophic emergency.

16. Annual training for the organization's leadership on that organization's essential functions, including training on their continuity responsibilities.
17. Annual training for all staff who are expected to telework during a continuity activation regarding conducting essential functions from a telework site. Training must include accessing and using records, communications, and systems.
18. Annual training for all organization personnel designated within the orders of succession for 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.
19. Annual training for those officials listed within the delegations of authority on all pre-delegated authorities for making policy determinations and other decisions, at the headquarters, regional, field, and other organizational levels, as appropriate.
20. Periodic briefings to managers about the essential records program and its relationship to their essential records and business needs.

Exercises

An organization's exercise program must include and document:

21. Compliance with HSEEP, as appropriate.
 22. An annual opportunity for ERG members to demonstrate their familiarity with continuity plans and procedures and to demonstrate the organization's capability to continue its essential functions.
 - a. An annual exercise that incorporates the deliberate and preplanned movement of ERG members to an alternate site.
 - b. An annual opportunity to demonstrate intra- and interagency communications capabilities.
 - c. An annual opportunity to demonstrate that backup data and records required to support essential functions at alternate sites are sufficient, complete, and current.
 - d. An annual opportunity to demonstrate familiarity with and capability to continue essential functions from telework sites, if used as a continuity strategy.
 23. A biennial exercise for ERG members to demonstrate their familiarity with the reconstitution procedures to transition from a continuity environment to normal activities when appropriate.
 24. A biennial exercise for DERG members to demonstrate their familiarity with devolution procedures.
 25. All organizations within the National Capital Region must annually participate in the Eagle Horizon continuity exercise; provide FEMA-required planning and exercise reports; provide evaluators, data collectors, facilitators, controllers, and other exercise required personnel, as requested; develop internal exercise injects, as required; develop an internal Eagle Horizon after-action report (AAR); and incorporate findings into a CAP.
 26. A comprehensive debriefing or hotwash after each exercise, which allows participants to identify systemic weakness in plans and procedures and to recommend revisions to the organization's continuity plan.
-

27. A cycle of events that incorporates evaluations, AARs, and lessons learned into the development and implementation of a CAP.
28. A CAP to assist in documenting, prioritizing, and resourcing continuity issues across all continuity elements identified during TT&E, assessments, and emergency operations.

The CAP must:

- a. Identify continuity deficiencies and other areas requiring improvement.
- b. Provide responsibilities and a timeline for corrective action.

ANNEX L. DEVOLUTION OF CONTROL AND DIRECTION

Devolution planning supports overall continuity planning and addresses catastrophes and other all-hazards emergencies that render an organization's leadership and ERG members unavailable or incapable of performing its essential functions from either the organization's primary operating facility or alternate sites. The devolution option may be used when the organization's primary operating facility, alternate site, and/or staff are not available. A continuity plan's devolution option addresses how an organization will identify and transfer responsibility for the performance of essential functions to personnel at a location that offers a safe and secure environment in which essential functions can continue.

The ultimate goal of both continuity and devolution planning is to continue the organization's essential functions. In that respect, the devolution counterpart must have the capability to perform an organization's essential functions within 12 hours for PMEFs and within the acceptable recovery time determined for other essential functions. Therefore, when choosing a devolution site, organizations must consider the capabilities of the site to ensure it has the communications, systems, equipment and resources pre-positioned or available within the accepted timeframe to continue essential functions. Requirements for devolution sites are primarily found in Annex G of this FCD.

Personnel stationed at the devolution site who are identified to conduct essential functions are referred to as the DERG. The organization must prepare these individuals to conduct the organization's essential functions. Organizations can support this process through the use of training and job aids, including standard operating procedures, desk guides, and handbooks. Requirements for DERG personnel are primarily found in Annex J and Annex K of this FCD.

Because of the requirements upon the transferring organization, the devolution site, and the DERG, the transferring organization and its chosen devolution counterpart must work closely together to fulfill devolution requirements. While it is the responsibility of the originating organization to ensure its essential functions are continued under all circumstances, including ensuring the devolution site is capable and the DERG is trained, the devolution site and DERG play a key role in ensuring requirements are met, as they are ultimately responsible for performing essential functions when the devolution option is activated.

Organizations may activate their devolution option as a continuity measure or as a temporary transfer of control as ERG members relocate to the alternate site. Additionally, organizations may choose to partially devolve, by transferring responsibilities for select essential functions, or devolve to multiple devolution sites, by transferring responsibilities for different essential functions to various sites.

REQUIREMENTS FOR DEVOLUTION OF CONTROL AND DIRECTION:

1. Organizations must develop a devolution option for continuity to address how it will identify and conduct its essential functions when the primary operating facility, alternate site, and/or ERG members are not available.

2. Organizations must address the following elements of a viable continuity capability in their devolution option: program plans and procedures, risk management, budgeting and acquisitions, essential functions, orders of succession and delegations of authority specific to the devolution site, continuity communications, essential records management, human resources, TT&E, and reconstitution.
3. For each identified essential function, organizations must determine the necessary resources to facilitate those functions' immediate and seamless transfer to the devolution site.
4. Organizations must include a roster that identifies fully trained DERG members stationed at the designated devolution site who have the authority to perform essential functions when the devolution option of the continuity plan is activated.
5. Organizations must identify what would likely activate or "trigger" the devolution option.
6. Organizations must specify how and when direction and control of organization operations will be transferred to and from the devolution site.
7. Organizations must list the necessary resources, such as equipment and materials, to facilitate the performance of essential functions at the devolution site.
8. Organizations must establish and maintain reliable processes and procedures for acquiring the resources necessary to continue essential functions and to sustain those operations for extended periods.
9. Organizations must establish and maintain procedures in order to transition responsibilities to personnel at the primary operating facilities upon termination of devolution.

ANNEX M. RECONSTITUTION OPERATIONS

Reconstitution requirements address the need for organizations to identify, develop, and coordinate a plan to return to normal operations once leadership determines that the actual emergency, or the threat of an emergency, is over. Just as an organization's capability to perform its essential functions rests upon the four pillars of continuity – leadership, staff, communications, and facilities – an organization's capability to reconstitute also rests on these pillars. Communication enables an organization to inform all personnel that the necessity for continuity operations no longer exists and to instruct personnel on how to resume normal operations. The non-ERG staff augments the ERG staff to begin the process of resuming non-essential functions. Leadership determines priorities and supervises the orderly return to normal operations. Organizations assess the status of affected facilities and transition back into the primary operating facility or a new facility.

As an element of continuity, reconstitution must be considered an essential function that ensures the continued support of other essential functions and the restoration of full normal operations. Since the process of reconstitution begins at the start of a continuity event, organizations should consider identifying a Reconstitution Team with leadership, staff, and resources dedicated and separate from existing essential function support to resume normal operations as quickly as possible. As detailed in NSPD-51/HSPD-20, DHS/FEMA serves as the President's lead agent for coordinating overall continuity operations and activities. In addition, GSA, OPM, and NARA also play key roles in reconstitution operations.

REQUIREMENTS FOR RECONSTITUTION OPERATIONS:

1. Organizations must develop a plan and provide the ability to recover from the effects of an emergency and for transitioning back to efficient normal operational status from continuity operations, once a threat or disruption has passed. This plan must:
 - a. Determine how the organization will assess the status of affected organization personnel, assets, and facilities;
 - b. 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, when appropriate;
 - c. Outline the necessary procedures for conducting a smooth transition from the continuity facility to either the normal primary operating facility, another temporary facility, or a new permanent facility;
 - d. Detail how the organization will inform all personnel that the actual emergency, or the threat of an emergency, and the necessity for continuity operations no longer exists, and instruct personnel on how to resume normal operations.
 - e. Detail how the organization will verify operational capability and availability, including systems, communications, essential records, infrastructure, and other required resources, and that the organization is fully capable of accomplishing all essential functions and operations at the new or restored facility.
 - f. Identify how the organization will determine which (if any) records were affected by the incident and ensure an effective transition or recovery of essential records and databases and other records that had not been designated as essential records.

2. Organizations must coordinate and pre-plan options for organization reconstitution regardless of the level of disruption that originally prompted the organization to implement its continuity plans.
3. Organizations must designate a Reconstitution Manager and a Devolution Reconstitution Manager (if the primary reconstitution manager is located at the primary operating facility) to oversee all phases of the reconstitution process.
4. In order to assist in the scoping of U.S. Government reconstitution plans and active programs, organizations are required to internally identify and document all perceived reconstitution needs via completion and submission of SF-2050, "Reconstitution Questionnaire." Organizations can centrally download and submit this form via classified systems at <https://gsapergamum.gold.ic.gov>. Organizations without access to classified systems can access this form via unclassified means at gsa.gov/forms and submit via classified fax at 202-501-1068. Organizations are required to annually review and re-submit the SF-2050. Organizations may contact GSA's Office of Emergency Response and Recovery at eoc@gsa.gov and/or 202-501-0012 for further instructions.

ANNEX N. CONTINUITY PLAN OPERATIONAL PHASES AND IMPLEMENTATION

A continuity plan is implemented to ensure the continuation or rapid resumption of essential functions during a continuity event. The continuity implementation process includes the following four phases: readiness and preparedness, activation, continuity operations, and reconstitution.

Readiness and Preparedness

Readiness is the ability of an organization to respond to a continuity activation. Although readiness is a function of planning and training, it is ultimately the responsibility of an organization's leadership to ensure that an organization can perform its essential functions before, during, and after all-hazards emergencies or disasters. This phase includes all organization continuity readiness and preparedness activities including the development, review, and revision of plans, TT&E, and risk management.

Non-HQ organizations may consider creating a "continuity readiness posture" similar to the executive branch's COGCON system for federal HQ entities, which is presented in Figure 5 on the next page.

EXECUTIVE BRANCH CONTINUITY OF GOVERNMENT READINESS CONDITIONS (COGCON) MATRIX

Readiness Level	Department & Agency (D/A)			Continuity Capability		
	Operations	Staffing Level	Time to Transition to Successive Stages	Communications	Succession	Impact on Departments & Agencies
COGCON 4	<ul style="list-style-type: none"> Continue to perform headquarters 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 Test, Training, and Exercise (TTE) plan(s) to ensure personnel readiness 	<ul style="list-style-type: none"> No staffing required at alternate operating facility(ies) Maintain normal delegations and devolution of authority to ensure performance of essential functions to respond to a no-notice event 	<ul style="list-style-type: none"> Continuity plan is fully operational within 12 hours 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> No special measures to protect or track the location of agency leadership and successors Ensure delegations of authority to lead departments and agencies are in place for senior personnel located outside of the National Capital Region 	<ul style="list-style-type: none"> No additional requirements
COGCON 3	<ul style="list-style-type: none"> Continue to perform headquarters 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) 	<ul style="list-style-type: none"> No staffing required 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 respond to a no-notice event 	<ul style="list-style-type: none"> Continuity plan is fully operational within 8 hours 4 hours to COGCON 2 	<ul style="list-style-type: none"> Conduct at least one additional internal agency communications test between normal operating locations (HQ and other) and alternate operating facility(ies) within 24 hours 	<ul style="list-style-type: none"> Track the locations of agency leaders and their successors on daily basis 	<ul style="list-style-type: none"> Additional staff time for communications testing and tracking agency leadership Potential shorter response times for basic staffing of alternate facility(ies)
COGCON 2	<ul style="list-style-type: none"> Continue to perform headquarters 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 	<ul style="list-style-type: none"> Deploy sufficient staff to alternate operating facility(ies) to allow activation with 4 hours notice 	<ul style="list-style-type: none"> Continuity plan is fully operational within 4 hours 4 hours to COGCON 1 	<ul style="list-style-type: none"> 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 communications tests at all alternate operating facility(ies) with applicable interagency partners within 48 hours and repeat not less than weekly 	<ul style="list-style-type: none"> Track the locations of agency leaders and their successors on daily basis Ensure at least one headquarters-level agency successor is out of the National Capital Region at all times 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Continue to perform headquarters 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 	<ul style="list-style-type: none"> Deploy sufficient staffing to alternate operating facility(ies) to perform essential functions with no notice 	<ul style="list-style-type: none"> Agency headquarters continuity plan activated immediately and report operational status within two hours 	<ul style="list-style-type: none"> Test internal agency communications between normal operating locations (HQ and other) and alternate operating facility(ies) daily Conduct communications tests at all alternate operating facility(ies) with applicable interagency partners daily 	<ul style="list-style-type: none"> Track the locations of agency leaders and their successors on a daily basis At least one headquarters-level agency successor must be at alternate operating facility(ies) 	<ul style="list-style-type: none"> Some agency leaders work from alternate facility(ies) Significant number of staff are required to work from alternate location(s)

Figure 5: COGCON Matrix

Activation (0-12 Hours)

This phase should include the activation of plans, procedures, and schedules for the continuation of essential functions, as well as for the personnel, essential records and databases, and equipment involved with these functions, with minimal disruption.

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

1. An organization receives or the region in which the organization is located receives notification of a credible threat, which leads the organization to enhance its readiness posture and prepare to take actions as necessary;
2. An organization experiences an emergency or a disruption that requires the relocation of ERG members to an alternate site;
3. An organization's ERG and/or primary operating facility and alternate site are unavailable or inaccessible, necessitating a shift of operations to a devolution site; and
4. Many, if not all, organizations must evacuate the immediate or larger geographically affected area.

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; and
7. Identifying available leadership.

Continuity Operations

This phase includes the following activities to continue essential functions:

1. Accounting for all organization personnel;
2. Reporting on operational capabilities to the FEMA Operations Center (FOC);
3. Performing essential functions;
4. Establishing communications with supporting and supported organizations, customers, and stakeholders; and
5. Preparing for the reconstitution of the organization.

Reconstitution

Leadership communicates instructions for resumption of normal operations to all staff, including supervising an orderly return to the normal operating facility, moving to another temporary facility, or 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 affected 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.

REQUIREMENTS FOR OPERATIONAL PHASES AND IMPLEMENTATION:

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

1. Follow procedures for the readiness and preparedness phase within its continuity plan and procedures.
2. Follow procedures for plan implementation, including using its decision matrix for continuity plan activation.
3. Alert and notify the following of continuity plan activation:
 - a. All staff (ERG, non-ERG, and DERG, if applicable);
 - b. Continuity facilities and on-site support teams;
 - c. Interdependent agencies; and
 - d. Other points-of-contact, stakeholders, vendors, and customers.
4. Report continuity activation status.
 - a. Non-HQ organizations must notify their HQ upon activation of continuity plans.
 - b. Upon activation of continuity plans at any level or location, organizations HQ points-of-contact (POCs) must notify FEMA's Continuity Readiness Cell (CRC) and submit a Continuity Status Reporting Form (or devolution as appropriate) using the form and procedures provided by FEMA NCP at the time of execution or activation of call-down procedures. The CRC will collate this information into the RRS.
5. Follow procedures for the relocation of ERG members and essential records to the alternate sites 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 DERG members at the devolution site.
8. Transition responsibilities from the primary operating facility to deployed ERG members at the alternate site or DERG members at the devolution site.
9. Account for all staff.
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-ERG personnel.
13. Identify and alert replacement personnel and augmentees, as necessary.
14. Perform PMEFS within 12 hours after an event and all other essential functions within the recovery time objective identified, under all threat conditions, from its

- continuity facilities (alternate sites or devolution sites), including the ability to maintain this capability until normal business activities can be 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 access to 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 needed to support and continue essential functions and sustain operations that are not already in place.
 16. Comply with any additional continuity reporting requirements from the FOC.
 17. Identify all available organization leadership at the continuity facilities 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 (i.e. labs or classified facilities);
 - c. Equipment and IT needs; and
 - d. Configuration of space (i.e. work areas, conference rooms, etc.).
 19. 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 all essential functions and operations at the new or restored primary operating facility.
 20. 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 decision-makers of the status of repairs, including estimates of when the repairs will be completed.
 21. Inform all personnel that the actual emergency, or the threat of an emergency, and the necessity for continuity operations no longer exists, and instruct personnel on how to resume normal operations.
 22. Phase down continuity facility operations and supervise the return of operations, personnel, records, and equipment to the primary or other operating facility in a priority-based approach, when appropriate.
 23. Conduct a smooth transition from the continuity facility to either the normal operating facility or a move to another temporary facility or a new permanent primary operating facility.
 24. Determine which (if any) records were affected by the incident and ensure an effective transition or recovery of essential records and databases and other records that had not been designated as essential records.

25. If applicable, report reconstitution status to the National Security Staff through FEMA NCP via the RRS.
- a. Non-HQ organizations must notify their organization HQ upon reconstitution.
 - b. Upon reconstitution at any level or location, organization HQ POCs must notify FEMA NCP via the reconstitution status report form, using the procedures provided by FEMA NCP at the time of execution.
 - c. FEMA will coordinate with interagency partners to facilitate executive branch reconstitution.

ANNEX O. LIST OF ACRONYMS

AAR	After-Action Report
BIA	Business Impact Analysis
BPA	Business Process Analysis
CAP	Corrective Action Program
CCA	Continuity Communications Architecture
CI	Critical Infrastructure
COG	Continuity of Government
COGCON	Continuity of Government Readiness Conditions
COOP	Continuity of Operations
CRC	Continuity Readiness Cell
CWG	Continuity Working Group
DHS	Department of Homeland Security
DERG	Devolution Emergency Relocation Group
ECG	Enduring Constitutional Government
ERG	Emergency Relocation Group
FCD	Federal Continuity Directive
FEMA	Federal Emergency Management Agency
FOC	FEMA Operations Center
GETS	Government Emergency Telecommunications Service
GSA	General Services Administration
HQ	Headquarters
HSEEP	Homeland Security Exercise and Evaluation Program
HSPD	Homeland Security Presidential Directive
IT	Information Technology
MEF	Mission Essential Function
MOA/MOU	Memorandum of Agreement/Memorandum of Understanding
MYSPMP	Multi-Year Strategy and Program Management Plan
NCC	National Continuity Coordinator
NCP	National Continuity Programs
NCPIP	National Continuity Policy Implementation Plan
NCS	National Communications System
NEF	National Essential Function
NSPD	National Security Presidential Directive
OEP	Occupant Emergency Plan
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PMEF	Primary Mission Essential Function
POC	Point-of-Contact
RRS	Readiness Reporting System
SF	Standard Form
TT&E	Test, Training, and Exercise
WPS	Wireless Priority Service

ANNEX P. GLOSSARY

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

Agencies – Federal departments and agencies means those executive departments enumerated in 5 U.S.C. § 101, together with the 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 departments, agencies, commissions, bureaus, boards, and independent organizations are referred to in this document as “organizations.”

All-Hazards – The spectrum of all types of hazards including accidents, technological events, natural disasters, terrorist attacks, warfare, and chemical, biological including pandemic influenza, radiological, nuclear, or explosive events.

Alternate Sites – “Alternate sites” are locations, other than the primary facility, used to carry out essential functions by relocating ERG members following activation of the continuity plan. These sites refer to not only other facilities and locations, but also work arrangements such as telework and mobile work concepts.

Business Impact Analysis (BIA) – A method of identifying the effects 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 facilities inherent in the execution of a function or requirement.

Catastrophic Emergency – Any incident, regardless of location, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting population, infrastructure, environment, economy, or government functions.

Category – This term refers to the four categories of organizations listed in Annex A to NSPD-51/HSPD-20.

Cold Site – A facility that is not manned on a day-to-day basis by personnel from primary operating facility. Organizations may be required to pre-install telecommunication equipment and IT infrastructure upon selection/purchase and deploy designated IT essential personnel to the facility to activate equipment/systems before it can be used.

Communications – Voice, video, and data capabilities that enable the leadership and staff to conduct the mission essential functions of the organization. Robust communications help ensure that the leadership receives coordinated, integrated policy and operational advice and recommendations and will provide the ability for governments and the private sector to communicate internally and with other entities (including with other federal organizations, tribal, state, territorial, and local governments, and the private sector) as necessary to perform their essential functions.

Continuity – An uninterrupted ability to provide services and support, while maintaining organizational viability, before, during, and after an event.

Continuity Advisory Group – A sub-Continuity Policy Coordination Committee group focused on interagency implementation of continuity programs. The Group is comprised of Continuity Coordinators, or their designees, from Category I, II, III, and IV (identified in NSPD-51/HSPD-20) organizations. Key State and local government representatives from the National Capital Region, and representatives from the legislative and judicial branches are invited, as appropriate.

Continuity Capability – The ability of an organization to continue to perform its essential functions, using COOP and COG programs and continuity requirements that have been integrated into the organization’s daily operations, with the primary goal of ensuring the preservation of our form of Government under the Constitution and the continuing 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 Communications Architecture (CCA) – An integrated, comprehensive, interoperable information architecture, developed utilizing the OMB-sanctioned Federal Enterprise Architecture Framework, that describes the data, systems, applications, technical standards, and underlying infrastructure required to ensure that Federal Executive Branch organizations can execute their PMEFs and MEFs in support of NEFs and continuity requirements under all circumstances.

Continuity Coordinators – Senior accountable executive branch official at the assistant secretary or equivalent level who represents their department or agency on the Continuity Advisory Group, ensures continuity capabilities in the organization, and provides 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 the organization.

Continuity Facilities – The term “continuity facilities” is comprehensive, referring to both continuity and devolution sites where essential functions are continued or resumed during a continuity event. “Alternate sites” are locations, other than the primary facility, used to carry out essential functions by relocating ERG members following activation of the continuity plan. “Devolution sites” are locations used to carry out essential functions by devolving the essential functions to a geographically separated facility and staff (the DERG) following activation of the devolution plan. These sites refer to not only other facilities and locations, but also work arrangements such as telework and mobile work concepts.

Continuity of Government (COG) – A coordinated effort within each branch of Government (e.g., the Federal Government’s Executive Branch) to ensure that NEFs continue to be performed during a catastrophic emergency.

Continuity of Government Readiness Conditions (COGCON) – For the Federal Executive Branch, the COGCON system establishes readiness levels in order to provide a flexible and coordinated response to escalating threat levels or actual emergencies, focusing on possible threats to the National Capital Region. The COGCON system establishes, measures, and reports the readiness of executive branch continuity programs, which is independent of other Federal Government readiness systems.

Continuity of Operations (COOP) – An effort within individual organizations to ensure they can continue to perform their essential functions during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.

Continuity Manager – The senior continuity planner who manages day-to-day continuity programs, represents their department or agency on the Continuity Advisory Group and working groups, as appropriate, and reports to the Continuity Coordinator on all continuity program activities.

Continuity Personnel – Those personnel, both senior and core, who provide the leadership advice, recommendations, and functional support necessary to continue essential operations. Continuity personnel are referred to as ERG members.

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

Continuity Policy Coordination Committee – A committee established to comprehensively address national level continuity program coordination, integration, oversight, and management. This forum institutionalizes national security policy development, implementation, and oversight for continuity programs. The Committee serves in a continuity oversight and management role with membership at the assistant secretary level from the following organizations: the Office of the Vice President; the Homeland and National Security Councils; the White House Military Office; the Office of Management and Budget; the Office of Science and Technology Policy; the Departments of State, Treasury, Defense, Justice, and Homeland Security; the Director of National Intelligence; the Central Intelligence Agency; the Federal Bureau of Investigation; the United States Secret Service; FEMA; and the Joint Chiefs of Staff. Other observers may be invited to attend.

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 to document and track improvement actions for a program.

Critical Infrastructure (CI) – Critical infrastructure means the systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Delegation of Authority – Identification, by position, of the authorities for making policy determinations and decisions at HQ, regional and field levels, and all other organizational locations. Generally, pre-determined delegations of authority will take effect when normal channels of direction have been disrupted and will lapse when these channels have been reestablished.

Devolution – Devolution requires the transition of roles and responsibilities for performance of essential functions through pre-authorized delegations of authority and responsibility. The authorities are delegated from an organization’s primary operating staff to other employees internal or external to the organization in order to sustain essential functions for an extended period. Devolution is a continuity option instead of or in conjunction with relocation in order to ensure the continued performance of essential functions.

Devolution Emergency Relocation Group (DERG) – Personnel stationed at the devolution site who are identified to conduct essential functions.

Devolution Site – “Devolution sites” are locations used to carry out essential functions by devolving the essential functions to a geographically separated facility and staff (the DERG) following activation of the devolution plan. These sites refer to not only other facilities, but also work arrangements such as telework and mobile work concepts.

Drive-Away Kit – A kit prepared by, and for, an individual who expects to deploy to an alternate site 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 – Records that support the execution of an organization’s essential functions.

Emergency Plan – Also referred to as Occupant Emergency Plan or building closure plan. Common scenarios that would lead to the activation of these plans would be inclement weather, localized power outages, localized telecommunications outages, etc. These types of events are generally short term in nature, do not impact employees ability to telework, and may not require an organization to activate its continuity plan.

Emergency Relocation Group (ERG) – Staff assigned responsibility to continue essential functions from an alternate site in the event that their primary operating facilities are threatened or have been 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 with respect to the legislative and judicial branches and with proper respect for the constitutional separation of powers among the branches. The ECG effort is intended to preserve the constitutional framework under which the Nation is governed and the capability of all three branches of Government, during a catastrophic emergency, to execute their constitutional responsibilities and to provide for orderly successions, appropriate transitions of leadership, interoperability, and support of NEFs.

Essential Functions – Essential functions are 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 Essential Supporting Activities.

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 Plan Packet – An essential records plan packet is an electronic or hard copy compilation of key information, instructions and supporting documentation needed to access essential records in an emergency situation.

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

Federal Continuity Directive (FCD) – A document developed and promulgated by DHS, 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.

Federal Executive Boards – A forum, established by Presidential Directive in 1961, for communication and collaboration among federal organizations outside of Washington, DC. With approximately 88 percent of all federal employees working outside of the National Capital Region, the national network of 28 Federal Executive Boards, located in areas of significant federal populations, serves as a cornerstone for strategic partnering in Government.

FEMA Operations Center (FOC) – A continuously operating entity of DHS, which is responsible for monitoring emergency operations and promulgating notification of changes to COGCON status.

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 of organizations, as defined by the Constitution, statute, regulation, presidential direction or other legal authorities, and the functions of the legislative and judicial branches. These functions are activities that are conducted to accomplish an organization’s mission and serve its stakeholders.

Headquarters (HQ) - In this FCD, the term “headquarters” refers to the central, head offices of operations for organizations identified in Annex A of NSPD-51/HSPD-20.

Homeland Security Exercise and Evaluation Program (HSEEP) – A capabilities-based and performance-based program that furnishes standardized policies, doctrines, and terminologies for the design, development, performance, and evaluation of homeland security exercises. The National Exercise Program uses the HSEEP as a common methodology for exercises. HSEEP also provides tools and resources to facilitate the management of self-sustaining homeland security exercise programs.

Hot Site – A continuity facility that already has in place the computer, telecommunications, other information technology, environmental infrastructure, and personnel required to recover critical business functions or information systems.

Interagency Board – A working group established by the NCC to review and recommend validation of potential PMEFs submitted by organizations for submission to the NCC for final approval.

Interoperability – “Interoperability” has two meanings: (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; (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.

Interoperable Communications – Communications that provide the capability to perform essential functions, in conjunction with other organizations, under all conditions.

Leadership – The senior decisionmakers who have been elected (e.g., the President, State governors) or designated (e.g., Cabinet Secretaries, chief executive officers) to head a branch of Government or other organization. Depending on the organization, directors and managers may also serve to assist in guiding the organization and making decisions.

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 limited set of organization-level government functions that must be continued throughout, or resumed rapidly after, a disruption of normal activities.

Multi-Year Strategy and Program Management Plan (MYSPMP) – A plan that guides the development of the continuity program over a set number of years via 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 here after 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 eleven local jurisdictions in the State of Maryland and the Commonwealth of Virginia.

National Communications System (NCS) – A system governed by Executive Order 12472 and comprised of the telecommunications assets of 24 organizations. DHS serves as the Executive Agent for the NCS, which is responsible for assisting the President, the National Security Council, the Director of Office of Science and Technology Policy, and the Director of OMB in (1) the exercise of telecommunications functions and their associated responsibilities and (2) the coordination of planning for providing the Federal Government, under all circumstances (including crises and emergencies, attacks, and recovery and reconstitution from those events), with the requisite national security and emergency preparedness communications resources.

National Continuity Coordinator (NCC) - The Assistant to the President for Homeland Security and Counterterrorism is the NCC. 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 National Essential Functions under all conditions (NSPD 51/HSPD 20, *National Continuity Policy*).

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

National Exercise Program – The Nation’s overarching exercise program executed by federal interagency partners. All interagency partners have adopted HSEEP as the methodology for all exercises that will be conducted as part of the Program.

Normal Operations – Generally and collectively, “normal operations” refer to the broad functions undertaken by an organization when it is assigned responsibility for a given functional area; these functions include day to day tasks, planning and execution of tasks.

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 would be inclement weather, fire, localized power outages, and localized telecommunications outages. These types of events are generally short-term in nature.

Orders of Succession – Orders of succession are a formal, sequential listing of organization positions (rather than specific names of individuals) that identify who is authorized to assume a particular leadership or management role under specific circumstances.

Organization Head – The highest-ranking official of the organization, or a successor or designee who has been selected by that official.

Organizations – Those executive departments enumerated in 5 U.S.C. § 101, together with the 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 departments, agencies, commissions, bureaus, boards, and independent organizations are referred to in this document as “organizations.”

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 the achievement of one or more objectives or goals.

Primary Mission Essential Functions (PMEFs) – Those organization MEFs, validated by the NCC, which must be performed in order to support the performance of NEFs before, during, and in the aftermath of an emergency. PMEFs need to be continuous or resumed within 12 hours after an event and maintained for up to 30 days or until normal operations can be resumed.

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 way, 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 in the program.

Readiness Reporting System (RRS) – A DHS program to collect and manage continuity capability data and assessments of executive branch organizations and their status to perform their PMEFs in support of the NEFs. The RRS will be used to conduct assessments and track 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 organization operations from the original or replacement primary operating facility.

Recovery – The implementation of prioritized actions required to return an organization's processes and support functions to operational stability following an interruption or disaster.

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

Resilience – The ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies.

Rights and Interests Records – Records that are necessary to protect the legal and financial rights of both the Federal Government and the persons who are affected by its actions.

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 – Risk management is 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.

Survivable Communications – The establishment and maintenance of an assured end-to-end communications path during all phases of an all hazard event.

Telecommuting Locations – Those locations equipped with computers and telephones that enable employees to work at home or at a location closer to their home than their main office.

Telework – A work flexibility arrangement under which an employee performs the duties and responsibilities of such employee’s 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.

Tests, Training, and Exercises (TT&E) – Measures to ensure 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. TT&E activities are designed to familiarize, impart skills and ensure viability of continuity plans.

Warm Site – A continuity facility that is equipped with some computer, telecommunications, other information technology, and environmental infrastructure, which is capable of providing backup after additional personnel, equipment, supplies, software, or customization are provided.

Weapons of Mass Destruction – Weapons that are capable of killing many people and/or causing a high-order magnitude of destruction or weapons that are capable of being used in such a way as to cause mass casualties or create large-scale destruction. They are generally considered to be nuclear, biological, chemical, and radiological devices, but these weapons can also be high-yield explosive devices.

ANNEX Q. AUTHORITIES AND REFERENCES

The following are the authorities and references for this FCD.

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. § 404).
- 3) Telework Enhancement Act, (5 U.S.C. §§ 6501-6506).
- 4) Executive Order 12148, *Federal Emergency Management*, July 20, 1979, as amended.
- 5) Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, April 3, 1984, as amended.
- 6) Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities*, November 18, 1988, as amended.
- 7) Executive Order 13286, *Establishing the Office of Homeland Security*, February 28, 2003.
- 8) Presidential Policy Directive 8, *National Preparedness*, April 11, 2011.
- 9) National Security Presidential Directive 51/Homeland Security Presidential Directive 20, *National Continuity Policy*, May 9, 2007, as amended.
- 10) Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- 11) NCS Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, November 7, 2011.
- 12) National Continuity Policy Implementation Plan, August 2007.

REFERENCES:

- 1) 36 Code of Federal Regulations, Part 1236, *Electronic Records Management*, November 2009.
- 2) 44 Code of Federal Regulations, Part 3541, *Federal Information Security Act of 2002*.
- 3) Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.
- 4) DHS Risk Management Fundamentals: Homeland Security Risk Management Doctrine, April 2011.
- 5) DHS Security Risk Steering Committee, *DHS Risk Lexicon 2010 Edition*, September 2010.

- 6) FCD 2, *Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process*, February 2008.
- 7) HSEEP, *Volume I: HSEEP Overview and Exercise Program Management*, February 2007.
- 8) HSEEP, *Volume II: Exercise Planning and Conduct*, February 2007.
- 9) HSEEP, *Volume III: Exercise Evaluation and Improvement Planning*, February 2007.
- 10) Intelligence Community Standard Number 500-19, *Universal Access and Remote Access to TS/SCI Web Content and Services*, July 7, 2010.
- 11) 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.
- 12) OPM Guide to Telework in the Federal Government, April 2011.
- 13) OPM Washington, DC, Area Dismissal and Closure Procedures, December 2010.
- 14) OPM Handbook on Pay and Leave Benefits for Federal Employees Affected by Severe Weather Conditions or Other Emergency Situations, July 2007.
- 15) OPM Human Resources Flexibilities and Authorities in the Federal Government, January 2008.
- 16) National Exercise Program Implementation Plan, November 2011.
- 17) National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010.
- 18) National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Systems and Organizations*, August 2009.
- 19) NCS Directive 3-1, *Telecommunications Service Priority System for National Security Emergency Preparedness*, August 10, 2000.
- 20) NCS Handbook 3-10-1, *Guidance for Improving Route Diversity within Local Area Networks*, February 9, 2009.
- 21) NCS Manual 3-10-1, *Guidance for Implementing NCS Directive 3-10*, January 8, 2008.