



Federal Continuity Directive 1 (FCD 1)

Federal Executive Branch National Continuity Program and Requirements

February 2008



**Homeland
Security**



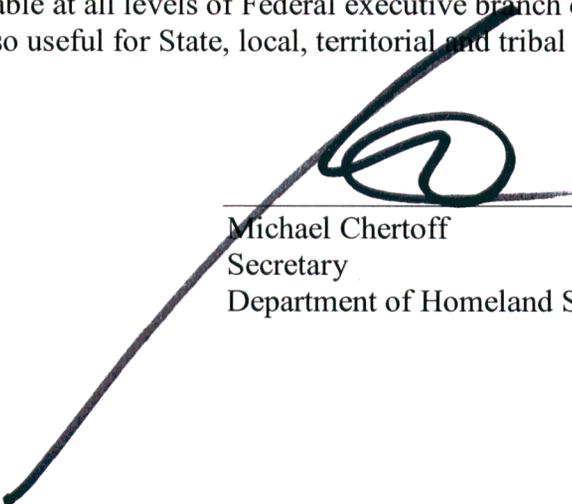
Homeland Security

In May 2007, the National Security Presidential Directive-51/Homeland Security Presidential Directive-20 (NSPD-51/HSPD-20) *National Continuity Policy* was issued by the President to establish and maintain a comprehensive and effective national continuity capability 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. In August 2007, the President approved the *National Continuity Policy Implementation Plan* to build upon the *Policy* and provide guidance to executive departments and agencies 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, has developed *Federal Continuity Directive 1 (FCD 1)*. The purpose of this FCD is to provide direction for the development of continuity plans and programs for the Federal executive branch. Effective continuity planning and programs 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 State, local, territorial and tribal 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, and are also useful for State, local, territorial and tribal governments and the private sector.



Michael Chertoff
Secretary
Department of Homeland Security

TABLE OF CONTENTS

1.	PURPOSE	1
2.	APPLICABILITY AND SCOPE	1
3.	SUPERSESSION	1
4.	AUTHORITIES.....	1
5.	REFERENCES	1
6.	POLICY.....	1
7.	BACKGROUND.....	2
8.	PROGRAM MANAGEMENT	3
9.	ELEMENTS OF A VIABLE CONTINUITY CAPABILITY	7
10.	COORDINATION WITH STATE, LOCAL, TERRITORIAL, AND TRIBAL GOVERNMENTS, AND THE PRIVATE SECTOR	11
11.	CONTINUITY PLAN OPERATIONAL PHASES AND IMPLEMENTATION.....	12
12.	ROLES AND RESPONSIBILITIES.....	12
13.	POINT OF CONTACT	21
14.	DISTRIBUTION	21
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.	VITAL RECORDS MANAGEMENT	I-1
ANNEX J.	HUMAN CAPITAL.....	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



Homeland
Security

FEDERAL CONTINUITY DIRECTIVE 1 (FCD 1)

Number	Date	Office
FCD 1	February 2008	FEMA National Continuity Programs

TO: HEADS OF FEDERAL DEPARTMENTS AND AGENCIES

SUBJECT: FEDERAL EXECUTIVE BRANCH NATIONAL CONTINUITY PROGRAM

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:** The provisions of this FCD are applicable to the executive departments enumerated in 5 U.S.C. § 101, including the Department of Homeland Security, 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, and independent organizations are hereinafter referred to as “agencies.” The continuity program elements outlined herein are for use at all levels of Federal executive branch organizations regardless of their location, and are also useful reference documents for non-Federal Government and private sector entities.
3. **SUPERSESION:** The provisions of this FCD supersedes:
 - a. Federal Preparedness Circular 60, *Continuity of the Executive Branch of the Federal Government at the Headquarters Level During National Security Emergencies*, and
 - b. Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations*, June 15, 2004.
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 (National Security Presidential Directive (NSPD)-51/Homeland Security Presidential Directive (HSPD)-20, *National Continuity Policy*). Continuity requirements must be incorporated into

the daily operations of all agencies to ensure seamless and immediate continuation of Primary Mission Essential Function (PMEF) capabilities so that critical government functions and services remain available to the Nation's citizens. Continuity planning will occur simultaneously with the development and execution of Federal agency 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 which is composed of efforts within individual agencies to ensure that their Mission Essential Functions (MEFs) continue to be performed 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 emergency delegations of authority, provide for the safekeeping of vital records, identify a range of continuity facilities and locations, provide for interoperable communications, provide for human capital planning, validate these capabilities through tests, training, and exercises (TT&E), specify a devolution of control and direction, and provide for reconstitution. All agencies, regardless of their size or location, shall have in place a viable continuity capability to ensure continued performance of their agency'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 asymmetric 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 agencies to continue their essential functions across a broad spectrum of emergencies. This, coupled with the potential for terrorist use of weapons of mass destruction (WMDs), has emphasized the importance of continuity programs that ensure continuity of essential government functions throughout the Federal executive branch.

Historically, the Federal Government has defined continuity efforts using the terms "COOP," "COG," and "ECG," as defined in Figure 1.

"**COOP**," or **Continuity of Operations**, is an effort within *individual* organizations (i.e., Federal executive branch departments and agencies) 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* (“*Policy*”) in NSPD-51/HSPD-20, which sets 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, 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 agency. It must be fully integrated into all aspects of an organization’s daily operations, thus creating a “culture of continuity.”

8. **PROGRAM MANAGEMENT**: An organization’s resiliency is directly related to the effectiveness of its continuity capability. An organization’s continuity capability—its ability to perform its essential functions continuously—rests upon key components and pillars, which are in turn built on the foundation of continuity planning and program management. These pillars are Leadership, Staff, Communications, and Facilities. The continuity program staff within an agency shall coordinate and oversee the development and implementation of continuity plans and supporting procedures.

Pillars 1 and 2: People – Leadership and Staff

Continuity of leadership is critical to ensure continuity of essential functions. Organizations must provide for a clear line of succession in the absence of existing leadership and the necessary delegations of authority to ensure that succeeding leadership has the legal authorities to carry out their duties. Continuity of leadership during crisis, especially in the case of senior positions like the President and heads of agencies, is important to reassure the Nation and give confidence to its citizens that the principal or appropriate successor is managing the crisis and ensuring the performance of essential functions. Leaders are needed to set priorities and keep focus.

Leaders and staff must be sufficiently trained to be able to perform their duties in a continuity environment. To ensure that required skill sets are available, personnel should be both cross-trained and vertically trained to be able to perform the functions of their peers and the persons above and below them in an emergency.

Pillar 3: Communications and Technology

The capability to communicate is critical to daily operations and absolutely essential in a crisis. The Nation’s domestic and international telecommunications resources, including commercial, private, and Government-owned services and facilities, are essential to support continuity plans and programs. All organizations must identify the communication requirements needed to perform their essential functions during both routine and continuity

conditions. Communication systems and technology must be interoperable, robust, and reliable. Planners must consider the resilience of their systems to operate in disaster scenarios that may include power and other infrastructure problems.

Organizations must use technology to perform essential functions as an intrinsic part of daily operations, utilizing voice, data, and video solutions as appropriate. Communications and business systems, including hardware and software for continuity operations, should mirror those used in day-to-day business to assist continuity leadership and staff in a seamless transition to crisis operations.

Pillar 4: Facilities

Facilities are the locations where essential functions are performed by leadership and staff. Organizations should have adequate, separate locations to ensure execution of their functions. Physical dispersion should allow for easy transfer of function responsibility in the event of a problem in one location.

Foundation: Continuity Planning and Program Management

While an organization needs leaders, staff, communications, and facilities to perform its essential functions, it also needs well thought out and detailed plans for what to do with those key resources. Planning must include all of the requirements and procedures needed to perform essential functions.

Other key continuity concepts include geographic dispersion, risk management, security, readiness and preparedness. Geographic dispersion of an organization's normal daily operations can significantly enhance the organization's resilience and reduce the risk of losing the capability to perform essential functions. Geographic dispersion of leadership, data storage, personnel, and other capabilities may be essential to the performance of essential functions following a catastrophic event and will enable operational continuity during an event that requires social distancing (e.g., pandemic influenza).

Risk management is the process to identify, control, and minimize the impact of uncertain events. Security is a key element to any continuity program to protect plans, personnel, facilities, and capabilities to prevent adversaries from interdicting continuity plans and operations. In order to ensure the safety and success of continuity operations, an effective security strategy must address personnel, physical, and information security.

Readiness is the ability of an organization to respond to an incident. While readiness is a function of planning and training, it is ultimately the responsibility of leadership to ensure an organization—through normal procedures or with a continuity plan—can perform its essential functions before, during, and after an incident. Federal and non-Federal Government (NFG) organizations outside the National Capital Region (NCR) may consider creating a “continuity readiness posture” similar to the executive branch's Continuity of Government Readiness Conditions (COGCON) system that 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 NCR (see Annex N). Other alert systems include Department of Homeland Security's (DHS) Homeland Security Advisory System

(HSAS), which provides guidance to the public on the status of our homeland security, and the United States Federal Response Stages for Pandemic Influenza.

Continuity Program Management Cycle

A standardized continuity program management cycle ensures consistency across all Federal Government continuity programs and supports the foundation and pillars that comprise the Nation's continuity capability. It establishes consistent performance metrics, prioritizes implementation plans, promulgates best practices, and facilitates consistent cross-agency continuity evaluations. Such a cyclic-based model that incorporates planning, training, evaluating, and the implementation of corrective actions, gives key leaders and essential personnel the baseline information, awareness, and experience necessary to fulfill their continuity program management responsibilities. The continuity program management cycle consists not only of its programmatic elements but also must include the plans and procedures that support implementation of the continuity program. These plans and procedures must also be evaluated pre- and post-event, tested or exercised, and assessed during the development of corrective action plans. Objective evaluations and assessments, developed from tests and exercises, provide feedback on continuity planning, procedures, and training. This feedback in turn supports a corrective action process that helps to establish priorities, informs budget decision making, and drives improvements in plans and procedures. This continuity program management cycle, as illustrated in Figure 2, should be used by all organizations as they develop and implement their continuity programs.

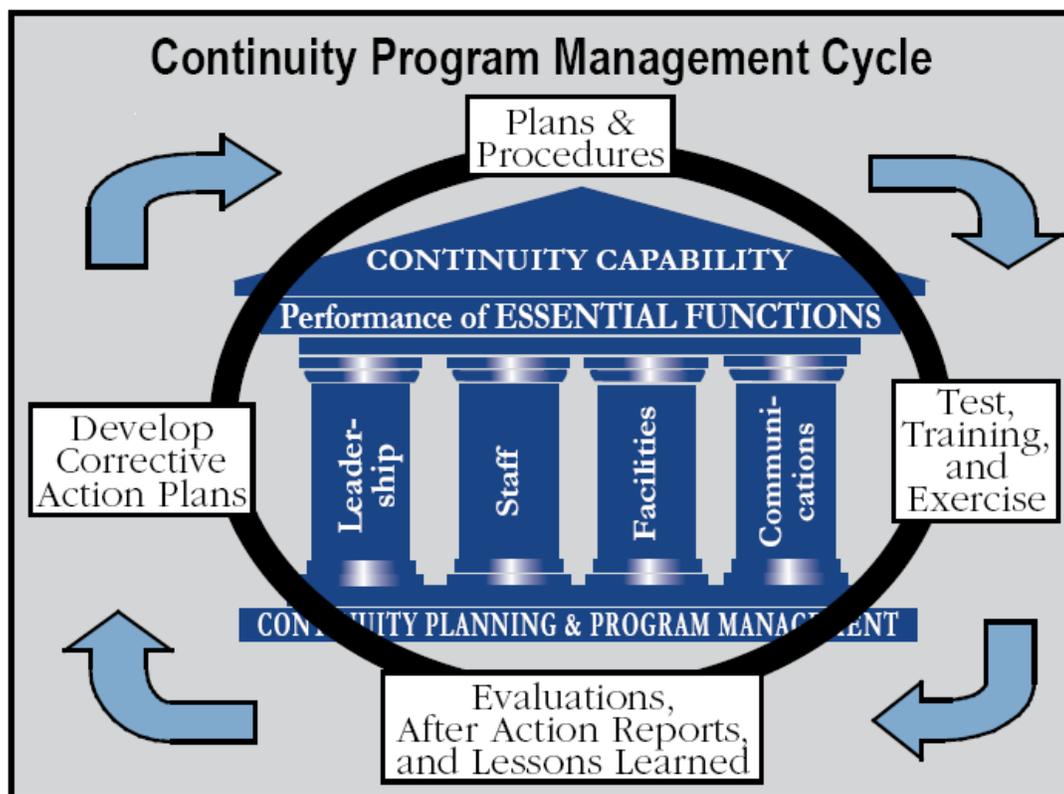


Figure 2

To support the continuity program management cycle, agencies will develop a continuity multiyear strategy and program management plan that provides for the development, maintenance, and annual review of continuity capabilities, requiring an agency to:

- a. Designate and review MEFs and PMEFs, as applicable.
- b. Define both short-term and long-term goals and objectives for plans and procedures.
- c. Identify issues, concerns, and potential obstacles to implementing the program, as well as a strategy for addressing these, as appropriate.
- d. Establish planning, training, and exercise activities, as well as milestones for accomplishing these activities.
- e. Identify the people, infrastructure, communications, transportation, and other resources needed to support the program.
- f. Forecast and establish budgetary requirements to support the program.
- g. Apply risk management principles to ensure that appropriate operational readiness decisions are based on the probability of an attack or other incident and its consequences.
- h. Incorporate geographic dispersion into the organization's normal daily operations, as appropriate.
- i. Integrate 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.
- j. Develop and implement a Corrective Action Program (CAP) that draws upon evaluations, after-action reports, and lessons learned from TT&E and real world events.

See Annex A – Program Plans and Procedures

Risk Management

The assessment and management of risk underlies the full spectrum of our national continuity program management, including decisions about when, where, and how to invest in resources that eliminate, control, or mitigate risks. In the face of multiple and diverse catastrophic possibilities, it is accepted that risk - a function of threats, vulnerabilities, and consequences - is a permanent condition. Therefore, a risk-based framework must be applied across all national continuity efforts in order to identify and assess potential hazards (including their downstream effects), determine what levels of relative risk are acceptable, and prioritize and allocate resources among all national continuity partners, both public and private, to ensure national continuity under all manner of incident conditions. Applying a disciplined approach to managing risk will help to achieve best progress, long term success, and overall effectiveness and efficiency.

See Annex B – Risk Management

Budgeting

Budgeting for and acquiring resources for continuity capabilities is one of the most important components of continuity planning. These budgetary requirements will directly support the ability of subordinate components and of regional- and field-level offices 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 agencies. These requirements are discussed in more depth in the “Key Considerations and Concept of Operations” section of the National Continuity Policy Implementation Plan. These “key 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 agency’s efforts in all other planning and preparedness areas. 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 agency will likely be limited, and therefore the agency 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 agency’s essential functions. These essential functions are then used to identify supporting tasks and resources that must be included in the agency’s continuity planning process.

The National Continuity Policy Implementation Plan has established three categories of essential functions: NEFs, PMEfs, and MEFs. The ultimate goal of continuity in the executive branch is the continuation of NEFs. To achieve that goal, the objective for executive agencies 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 **National Essential Functions (NEFs)** (listed in Annex D of this document) represent the overarching responsibilities of the Federal Government to lead and sustain the Nation and will be the primary focus of the Federal Government’s leadership during and in the aftermath of an emergency.

Primary Mission Essential Functions (PMEfs) are those agency MEFs that must be performed to support or implement the performance of the NEFs before, during, and in the aftermath of an emergency. PMEfs are defined as those functions that need to be continuously performed during an event or resumed within 12 hours of an event, and that need to be maintained for up to 30 days after an event or until normal operations can be resumed.

Mission Essential Functions (MEFs) are a broader set of essential functions that includes not only an agency’s PMEfs, but also all other agency functions that must be continued throughout or resumed rapidly after a disruption of normal activities but that do not rise to the level of being 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 during disruption of normal operations.

When identifying an agency’s essential functions and categorizing them as MEFs or PMEfs, organizations with incident management responsibilities must be sure to incorporate these

into their continuity planning requirements for performing these functions. Integration of continuity planning with incident management planning and operations include responsibilities delineated in the National Response Framework (NRF) and is linked to an organization's ability to conduct its PMEFs.

See Annex D – Essential Functions

b. ORDERS OF SUCCESSION. Agencies are responsible for establishing, promulgating, and maintaining orders of succession to key positions. Such orders of succession are an essential part of an agency's continuity plan to ensure that agency personnel know who assumes the authority and responsibility of the agency's leadership if that leadership is incapacitated or becomes otherwise unavailable during a continuity situation. Orders should be of sufficient depth to ensure that the agency can manage and direct its essential functions and operations while remaining a viable part of the Federal Government throughout any emergency.

See Annex E – Orders of Succession

c. DELEGATIONS OF AUTHORITY. To ensure a rapid response to any emergency requiring the implementation of its continuity plan, an agency should delegate authorities for making policy determinations and other decisions, at the headquarters (HQ), field, satellite, and other organizational levels, as appropriate. It is vital to clearly establish delegations of authority, so that all agency personnel know who has the right to make key decisions during a continuity situation. 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. As part of their continuity planning, all agencies must identify alternate facilities; alternate uses for existing facilities; and as appropriate, virtual office options including telework. Risk assessments will be conducted on these facilities to provide reliable and comprehensive data to inform risk mitigation decisions that will allow agencies to protect assets, systems, networks, and functions while determining the likely causes and impacts of any disruption. All agency personnel shall be briefed on agency continuity plans that involve using, or relocating personnel to alternate facilities, existing facilities, or virtual offices. Continuity personnel must be provided supplemental training and guidance on relocation procedures.

See Annex G – Continuity Facilities

e. CONTINUITY COMMUNICATIONS. The ability of an agency to execute its essential functions at its continuity facilities depends on the identification, availability, and redundancy of critical communications and information technology (IT) systems to support connectivity among key government leadership personnel, internal agency elements, other agencies, critical customers, and the public, during crisis and disaster conditions. The capabilities of communications and IT systems (e.g., secure and nonsecure voice systems, video conferencing, and fax and other messaging capabilities) to be used during an incident

should mirror those capabilities used during day-to-day operations, and the choice of communications and IT systems should consider how resilient those systems are and how capable they are of operating under conditions that may involve power or other infrastructure disruptions. All necessary and required communications and IT capabilities must be operational as soon as possible following a continuity activation, and in all cases within 12 hours of continuity activation. Agencies need to plan accordingly for essential functions that require uninterrupted communications and IT support.

See Annex H – CONTINUITY COMMUNICATIONS

f. VITAL RECORDS MANAGEMENT. Another critical element of a viable continuity plan and program includes 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 situation. Agency personnel must have access to and be able to use these records and systems to perform essential functions and to reconstitute back to normal agency operations. To ensure performance of essential functions, agencies will pre-position and regularly update duplicate Emergency Operating Records.

See Annex I – Vital Records Management

g. HUMAN CAPITAL.

Leadership and Staff. People are critical to the operations of any organization. Choosing the right people for an organization's staff is vitally important, and this is especially true in a crisis situation. Leaders are needed to set priorities and keep focus. During a continuity event, emergency employees and other special categories of employees will be activated by an agency to perform assigned response duties. One of these categories is continuity personnel, referred to as the Emergency Relocation Group (ERG) members.

Human Capital Considerations. An agency's continuity program, plans, and procedures should incorporate existing agency-specific guidance and direction for human capital management. These can include guidance on pay, leave, work scheduling, benefits, telework, hiring, etc., authorities and flexibilities. An agency's Continuity Coordinator (or continuity manager) should work closely with the agency's Chief Human Capital Officer or Director of Human Resources to resolve human capital issues related to a continuity event. Human capital issues can be solved typically at the agency level through the agency's Chief Human Capital Officer or Director of Human Resources, or their designees, using available laws, the U.S. Office of Personnel Management regulations and guidance, as well as agency implementing instructions.

The planning and preparedness related to leadership, staff, and human capital considerations for a continuity event encompasses the following six activities:

- 1) Agencies must develop and implement a process to identify, document, communicate with and train continuity personnel.
- 2) Agencies must provide guidance to continuity personnel on individual preparedness measures they should take to ensure response to a continuity event.

- 3) Agencies must implement a process to communicate the agency's operating status to all staff.
- 4) Agencies must implement a process to contact and account for all staff in the event of an emergency.
- 5) Agencies must identify a human capital liaison from the agency's human resources staff to work with the Continuity Coordinator or continuity manager when developing the agency's emergency plans.
- 6) Agencies must implement a process to communicate their human capital guidance for emergencies (pay, leave, staffing and other human resources flexibilities) to managers and make staff aware of that guidance in an effort to help agencies continue essential functions during an emergency.

See Annex J – Human Capital

h. TEST, TRAINING, AND EXERCISE (TT&E). An effective TT&E program is necessary to assist agencies to prepare and validate their organization's continuity capabilities and program and the Federal executive branch's ability to perform MEFs and PMEFs during any emergency. This requires the identification, training, and preparedness of personnel capable of performing their continuity responsibilities and implementing procedures to support the continuation of agency essential functions.

Training provides the skills and familiarizes leadership and staff with the procedures and tasks they must perform in executing continuity plans. Tests and exercises serve to assess and validate all the components of continuity plans, policies, procedures, systems, and facilities used to respond to and recover from an emergency situation and identify issues for subsequent improvement. All agencies must plan, conduct, and document periodic TT&Es 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 must be documented in an organization's CAP.

See Annex K – Test, Training, and Exercises

i. DEVOLUTION OF CONTROL AND DIRECTION. Devolution is the capability to transfer statutory authority and responsibility for essential functions from an agency's primary operating staff and facilities to other agency employees and facilities, and to sustain that operational capability for an extended period.

Devolution planning supports overall continuity planning and addresses the full spectrum of threats and all-hazards emergency events that may render an agency's leadership or staff unavailable to support, or incapable of supporting, the execution of the agency's essential functions from either its primary location or its alternate location(s). Agencies shall develop a devolution option for continuity, to address how those agencies will identify and conduct its essential functions during an increased threat situation or in the aftermath of a catastrophic emergency.

See Annex L – Devolution of Control and Direction

j. **RECONSTITUTION.** Reconstitution is the process by which surviving and/or replacement agency personnel resume normal agency operations from the original or replacement primary operating facility. Reconstitution embodies the ability of an agency to recover from an event that disrupts normal operations and consolidates the necessary resources so that the agency can resume its operations as a fully functional entity of the Federal Government. In some cases, extensive coordination may be necessary to procure a new operating facility, if an agency suffers the complete loss of a facility or in the event that collateral damage from a disaster renders a facility structure unsafe for reoccupation.

See Annex M – Reconstitution Operations

- 10. COORDINATION WITH STATE, LOCAL, TERRITORIAL, AND TRIBAL GOVERNMENTS, AND THE PRIVATE SECTOR:** The Federal Government’s NEFs, prescribed in NSPD-51/HSPD-20, cannot be performed without the robust involvement of NFGs and the private sector. State, local, territorial, and tribal 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, road construction, public education) continue on a daily basis. The Federal Government’s COOP, COG, and ECG plans and operations shall be appropriately integrated with the emergency and continuity plans and capabilities of State, local, territorial, and tribal governments, and private sector owners and operators of critical infrastructure, as appropriate, in order to promote interoperability and prevent redundancies and conflicting lines of authority.

Agencies should coordinate with regional entities, State, local, territorial, and tribal governments, and private sector owners and operators of the Nation’s critical infrastructure and key resources (CI/KR) as appropriate, to build relationships and ensure unity of effort by:

- a. Incorporating their capabilities into the agency’s continuity planning and exercise activities to the extent possible.
- b. Identifying hazards relevant to the agency’s mission and location.
- c. Partnering with these entities to develop continuity plans that are coordinated with Federal plans to the extent possible.
- d. Participating in continuity working groups (CWGs), information sharing, training, and exercises, as appropriate.
- e. Coordinating occupant emergency plans (OEPs), shelter-in-place plans, and regional and local evacuation plans.
- f. Participating in existing alert and notification networks and credentialing initiatives, as appropriate.
- g. Identifying interdependencies and ensuring resiliency with critical infrastructure and services at all levels.
- h. Coordinating continuity resource and security requirements, as appropriate.
- i. Working with organizations such as DHS/Federal Emergency Management Agency (FEMA) Regional/State-level CWGs, DHS/Office of Infrastructure Protection, and the various CI/KR Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs), Federal Executive Boards (FEBs) and Federal Executive Associations (FEAs) to augment and strengthen coordination efforts.
- j. Participating in other coordinating 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 event. Agencies should develop an executive decision-making process that allows for a review of the emergency and a determination of the best course of action based on the agency's readiness posture. An agency's continuity implementation process will include the following four phases: readiness and preparedness, activation and relocation, continuity operations, and reconstitution. The four phases are implemented as illustrated in Figure 3.

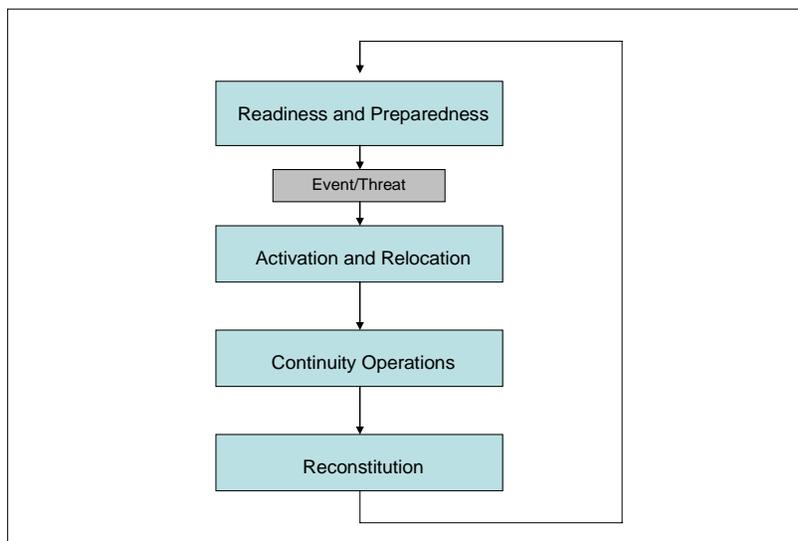


Figure 3

See Annex N – Continuity Plan Operational Phases and Implementation

12. ROLES AND RESPONSIBILITIES: The following responsibilities are assigned to the leadership or leadership of designated entities listed below, as outlined in the National Continuity Policy Implementation Plan.

- a. The President is responsible for leading the activities of the Federal Government for ECG.
- b. The National Continuity Coordinator (NCC) is responsible for:
 - 1) Providing continuity policy coordination among all agencies, monitoring performance, and reporting to the President as appropriate.
 - 2) Periodically reviewing and, as necessary, coordinating the revision of the NEFs.
 - 3) Overseeing the Continuity Policy Coordination Committee (CPCC), which was established consistent with HSPD-1 of October 29, 2001 (“Organization and Operation of the Homeland Security Council”). The CPCC is chaired by a designee of the NCC and is the main day-to-day forum for continuity policy coordination.
 - 4) Establishing a Continuity Advisory Group (CAG) as a sub-CPCC group focused on interagency implementation of continuity programs.

-
- 5) Establishing an interagency board (IAB), as a working group of the CPCC to review and recommend validation of potential PMEFs submitted by agencies for submission to the NCC for final approval.
 - 6) Within 30 days of IAB review, considering identified PMEFs for validation and approval.
 - 7) Coordinating with FEMA in developing a continuity assessment tool for the agencies to measure continuity readiness against requirements contained in NSPD-51/ HSPD-20 and reporting the continuity assessment results to the President.
 - 8) Within the annual budget process and on an ongoing basis, assisting OMB and agencies with continuity budget development and prioritization, including long-term equipment life cycle replacements and upgrades.
 - 9) On an ongoing basis, ensuring coordination of continuity acquisition functions with DHS and the General Services Administration (GSA).
 - 10) On an ongoing basis, coordinating the integration of national continuity test, training, and exercise programs.
 - 11) Annually submitting a report to the President that assesses (a) the ability of executive branch departments and agencies to perform their PMEFs, (b) the scope and effectiveness of legislative, executive, and judicial branch coordination, and the nature and level of executive branch support, to perform the NEFs and achieve common continuity goals, and (c) the scope and effectiveness of coordination among State, local, territorial, and tribal governments and the private sector to perform the NEFs and achieve common continuity goals.
 - 12) Coordinating, without exercising directive authority, the development and implementation of continuity policy for agencies.
 - 13) Maintaining and revising as necessary the various agency PMEFs and MEFs in order to meet requirements for continuity, including ECG, COG, and COOP.
- c. The Assistant to the President for National Security Affairs (APNSA) is responsible for coordinating with the NCC on the development and implementation of continuity policy for executive departments and agencies.
- d. The Secretary of Homeland Security is responsible for:
- 1) On an ongoing basis, serving as the President's lead agent for coordinating overall continuity operations and activities and domestic incident management of executive departments and agencies, and in such role performing the responsibilities set forth in NSPD-51/HSPD-20 and in HSPD-5.
 - 2) Coordinating the implementation, execution, and assessment of continuity activities and programs.
 - 3) Quarterly, ensuring FEMA's Continuity Coordinator chairs meetings of the CAG and reports to the CPCC.
 - 4) On an as-needed basis in coordination with the CAG and in consultation with the CPCC, developing and promulgating Federal Continuity Directives that establish
-

- continuity planning requirements, continuity plan templates, TT&E programs including required continuity training, types and frequency of exercises, and assessment criteria to ensure agencies develop and maintain a robust TT&E program.
- 5) In coordination with the CPCC, issuing FCDs on Continuity Requirements to include the formalized and standardized process for the identification of MEFs, and revising through annual or as needed Directives thereafter, and the identification and submission of potential PMEFs that are consistent and supporting of the NEFs for review by the IAB, consolidating the agencies' PMEFs, and compiling and submitting potential PMEFs to the NCC.
 - Include a standardized checklist to allow agencies to assess their PMEFs through a risk management process;
 - Include guidance on how the PMEF links to/supports NEF(s); and
 - Include guidance on impact statements if a specific PMEF is not conducted.
 - 6) Within 30 days after submission of agency MEFs and potential PMEFs, compiling submissions and providing them to the NCC for IAB review and validation.
 - 7) On an annual basis, developing, leading, and conducting an integrated COOP and COG continuity training exercise, incorporated into the National Exercise Program (NEP), and reporting the results to the NCC.
 - 8) Providing continuity direction, training, and coordination of continuity exercises, as well as providing continuity program and biennial assessments of department and agency continuity capabilities and reporting the results to the President through the NCC.
 - 9) Developing, leading, and conducting the Federal executive branch continuity training and exercise program, which shall be incorporated into the NEP developed pursuant to HSPD-8 of December 17, 2003 ("National Preparedness"), in consultation with an official designated by the Chief of Staff to the President.
 - 10) Coordinating the integration of Federal executive branch continuity plans and operations with State, local, territorial, and tribal governments and private sector owners and operators of critical infrastructure, as appropriate, in order to provide for the delivery of essential services during an emergency.
 - 11) On an ongoing basis, ensuring that the DHS National Operations Center (NOC), National Infrastructure Coordinating Center (NICC), and FEMA Operations Center (FOC) maintain 24-hour operations to ensure appropriate responses for continuity, incident management activities, and for emergency operations.
 - 12) On an ongoing basis, ensuring that the National Preparedness Goal, the Target Capabilities List, and State and Local Homeland Security Grant Programs criteria provide guidance to State, local, tribal and territorial governments on continuity priorities and implementation guidelines.
 - 13) On an ongoing basis, ensuring that DHS makes available continuity planning and exercise funding in the form of grants, as provided by law, to State, local, territorial, tribal governments and the private sector.

- 14) On an ongoing basis, ensuring that the National Infrastructure Protection Plan (NIPP) supports the Nation's continuity plans and programs and provides guidance to private sector entities and operators of CI/KR on continuity priorities and implementation guidelines.
- 15) Not less than quarterly, conducting assessments of continuity communications capabilities in consultation with an official designated by the Chief of Staff to the President.
- 16) Establishing a familiarization briefing on MEF and PMEF identification for agency Continuity Coordinators (Assistant Secretary-level).
- 17) Annually updating training courses for agency continuity planners on the identification and development of PMEFs and MEFs, in addition to maintaining ongoing continuity training courses.
- 18) Within 30 days after receipt of technical requirements from the Office of Science and Technology Policy (OSTP), as Executive Agent of the National Communications System (NCS), providing the Director of OSTP, and Department of Defense (DOD) with an implementation plan for a comprehensive Continuity Communications Architecture (CCA), which shall include the minimum requirements necessary to finalize selection of a secure communications system by DOD.
- 19) Within 90 days after receipt of technical requirements from OSTP, through the NCS, developing, implementing, and beginning maintenance of a comprehensive CCA.
- 20) On an as-needed basis, revising and promulgating integrated continuity planning guidance to NFGs and others as appropriate.
- 21) On an as-needed basis, providing critical infrastructure assistance and support in accordance with HSPD-7 and the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.
- 22) On an as-needed basis, providing cybersecurity assistance and support in accordance with HSPD-7 and the National Strategy to Secure Cyberspace.
- 23) Developing regional and State level CWGs to, at a minimum, conduct annual continuity conferences to address joint Federal and NFG continuity planning and other elements of a viable continuity program.
- 24) Developing and promulgating continuity planning guidance to State, local, territorial, and tribal governments. Guidance should include procedures and models for development of PMEFs, orders of succession, delegations of authority, devolution, reconstitution, establishment of alternate facilities, interoperable communications, the safeguarding of vital resources, facilities, and records, and a test, training, and exercise program that will ensure a viable continuity program.
- 25) Providing planning guidance to NFGs on development of internal MEFs. Guidance will be based on the requirement of continuing the performance of essential functions.
- 26) Providing critical infrastructure assistance and support for the Nation's continuity plans and programs in accordance with guidance in HSPD-7. Organizations established to support the NIPP will be members of and support the activities of the

-
- CWGs, including supporting the activities of the DHS/FEMA regional and State level CWGs.
- 27) Developing and promulgating continuity planning guidance for private sector critical infrastructure owners and operators. Guidance should be integrated into the NIPP and be supported by CI/KRs Coordinating Councils and Committees in accordance with guidance in HSPD-7.
 - 28) Inviting the private sector to participate in government training and exercises, where appropriate.
 - 29) Developing, operating, and maintaining a continuity Readiness Reporting System (RRS) which will measure and report both the individual and aggregate ability of agencies to continue their PMEFS in support of the required NEFs. This system identifies near real-time COOP and COG programmatic capabilities and requires monthly or as required data input from system users.
 - 30) Coordinating with the Assistant to the President for Homeland Security and Counterterrorism (APHS/CT) in developing a continuity assessment tool for the agencies to measure continuity readiness against requirements contained in NSPD-51/HSPD-20.
- e. Heads of Federal Government executive agencies are responsible for:
- 1) On an ongoing basis, ensuring performance of agency PMEFS.
 - 2) On an ongoing basis, incorporating continuity requirements into daily agency operations.
 - 3) On an ongoing basis, ensuring the agency has continuity plans for dealing with a national or localized emergency situation and ensuring the continued performance of all PMEFS in support of the NEFs, as well as continued performance of MEFs.
 - 4) Appointing a senior accountable official, at the Assistant Secretary or equivalent level, as the Continuity Coordinator for the department or agency.
 - 5) Annually submitting a report to the NCC certifying that the agency has a continuity capability plan that includes the items in Paragraph 11 of NSPD-51/ HSPD-20.
 - 6) On an ongoing basis, consistent with sections 11(e) and 19(c) of NSPD-51/ HSPD-20, planning, programming, and budgeting for secure continuity communications capabilities.
 - 7) Within 90 days after DHS's guidance, reviewing and revising MEFs and identifying and submitting potential PMEFS. To support the PMEF approval and implementation process, agency heads are responsible for:
 - a. Validating and approving their identified PMEFS and MEFs, as appropriate, and accompanying Business Process Analysis (BPAs).
 - b. Identifying and submitting to the NCC through the IAB their respective MEFs and potential PMEFS that support NEFs.
-

-
- c. After validation of agency PMEFS and annually thereafter, ensuring key leaders and support staff are provided familiarization training of agency PMEFS and MEFs.
 - d. After validation of agency PMEFS, ensuring PMEFS and MEF interdependencies are coordinated internally, at the interagency level, and with private sector partners.
 - e. In consultation with the NCC, periodically reviewing and revising their PMEFS and MEFs.
- 8) During development of PMEFS, coordinating and integrating with Federal and non-Federal Government organizations; State, local, tribal, and territorial governments; and private sector entities on those relevant activities essential to PMEFS and MEFs.
 - 9) On an ongoing basis, participating in DHS's NEP.
 - 10) On an ongoing basis, incorporating Office of Management and Budget (OMB) Circular A-11 guidance, or other OMB guidance on continuity as provided, when developing continuity budgets.
 - 11) As required, submitting Continuity Readiness Reports and other reports as requested, through the RRS.
 - 12) Developing a CAP to assist in documenting, prioritizing, and resourcing continuity issues identified during TT&E, assessments, and emergency operations.
 - 13) Planning, programming, and budgeting for continuity capabilities (including for planning, conducting, and supporting annual TT&E programs). For continuity funding requests, incorporate OMB guidance from Circular A-11, to ensure proper accounting of spending related to homeland security.
 - 14) Evaluating program readiness, to ensure the adequacy and capability of continuity plans and programs.
 - 15) Promulgating and disseminating continuity guidance to all subordinate elements including regional and field offices.
 - 16) Emphasizing geographic dispersion of leadership, staff, and infrastructure, as appropriate, in order to increase survivability and maintain uninterrupted Government functions.
 - 17) Executing continuity plans and complying with the requirements and assigned responsibilities under the COGCON program.
 - 18) Participating in and conducting testing, as appropriate, to ensure viability of communications systems.
- f. The Director of OMB is responsible for:
 - 1) As necessary, in coordination with the NCC, issuing continuity planning guidance for the development of continuity budget requests.
 - 2) Annually conducting an assessment of executive agency continuity funding requests and performance data that are submitted by executive branch agencies as part of the
-

-
- annual budget request process in order to monitor progress in the execution of the National Continuity Policy Implementation Plan and continuity budgets.
- 3) Annually reconciling agency continuity funding requests and performance data with Continuity Readiness Reporting and annual continuity assessments compiled by FEMA.
- g. The Director of OSTP is responsible for:
- 1) Annually reviewing and revising as required, minimum requirements for continuity communications for executive branch departments and agencies, in consultation with the APHS/CT, the APNSA, the Director of OMB, and the Chief of Staff to the President (as well as the Secretaries of Defense and Homeland Security).
 - 2) Establishing and chairing a Continuity Communications Architecture Board (CCAB).
 - 3) Within 30 days after validation of PMEFs, distributing requirements for, and updating as needed, a comprehensive CCA in consultation with the APHS/CT, the APNSA, the Director of OMB, and the Chief of Staff to the President (as well as the Secretaries of Defense and Homeland Security).
 - 4) On an ongoing basis, monitoring the development, implementation, and maintenance of a CCA to integrate continuity components, in consultation with the APHS/CT, the APNSA, the Director of OMB, and the Chief of Staff to the President (as well as the Secretaries of Defense and Homeland Security).
 - 5) Quarterly and annually, reviewing assessments of continuity communications capabilities and reporting the results and recommended remedial actions to the NCC.
- h. The Official Designated by the Chief of Staff to the President is responsible for:
- 1) On an ongoing basis, advising the President, Chief of Staff to the President, the APHS/CT, and the APNSA on COGCON operational execution options.
 - 2) On an ongoing basis, ensuring that the executive branch's COOP and COG policies, in support of ECG efforts, are appropriately coordinated with those of the legislative and judicial branches in order to ensure interoperability and allocate national assets efficiently to maintain a functioning Federal Government.
 - 3) On an ongoing basis, consulting with the Secretary of Homeland Security in order to ensure synchronization and integration of continuity activities among the four categories of executive agencies.
- i. The Secretary of Defense is responsible for:
- 1) Within 60 days after the publication by DHS of the CCA implementation plan, identifying the secure, integrated, COG communications for use by the President, the Vice President, and, at a minimum, Category I executive agencies.
 - 2) Upon identification and implementation, continuously maintaining the secure, integrated, COG communications for the President, the Vice President, and, at a minimum, Category I executive departments and agencies.
-

-
- 3) Not less than quarterly, assisting the Secretary of Homeland Security, and an official designated by the Chief of Staff to the President, with assessments of continuity communications capabilities.
 - 4) On an ongoing basis, assisting DHS in conducting continuity training and exercises and in providing assistance during emergencies and disasters.
- j. The Director of National Intelligence is responsible for:
- 1) Every two years, producing an assessment for the NCC of the foreign and domestic threats to the Nation's COG.
 - 2) On an ongoing basis, in coordination with the Secretary of Homeland Security and the Secretary of Defense, provide geospatial products to support continuity planning, training, and exercise activities.
 - 3) During emergencies and disasters, providing geospatial continuity operational support to DHS to assist in response and recovery operations.
- k. The Director of U.S. Office of Personnel Management (OPM) is responsible for:
- 1) Developing and promulgating personnel guidance to support Federal executive branch continuity plans and programs.
 - 2) Establishing telework guidance to support agency continuity programs.
 - 3) In coordination with the Secretary of Homeland Security, providing guidance to and coordinating with the FEBs to assist in facilitating planning meetings and exercises to develop effective continuity programs among participating Federal executive agencies and, where appropriate, NFGs, including respective State, local, territorial, and tribal governments and private sector owners and operators of critical infrastructure in their planning and preparedness activities.
 - 4) On an ongoing basis, assisting DHS in conducting continuity training, exercises, assessments, and other preparedness activities.
 - 5) Submitting a report to the NCC on the possibility of creating an occupational specialty for continuity and an associated training program, and, if approved, working with FEMA to include the information in a FCD.
 - 6) Assuring that FEBs assist and coordinate continuity efforts before, during, and after an emergency.
 - 7) Providing guidance to agencies on developing personnel policies that address continuity plans and procedures, including alternate work options.
- l. The Administrator of the GSA is responsible for:
- 1) On an ongoing basis, coordinating the provision of executive branch facilities to support continuity operations and maintaining the database for all agency alternate facilities.
 - 2) On an ongoing basis, facilitating a coordinated and seamless executive branch continuity infrastructure and providing and maintaining a centralized procurement system for all agency continuity infrastructure requirements.
-

-
- 3) On an ongoing basis, assisting the Secretary of Homeland Security in conducting continuity TT&Es, assessments, and other preparedness activities.
 - 4) During and in the aftermath of emergencies and disasters, assisting the Secretary of Homeland Security and affected agencies in their recovery and reconstitution.
- m. The Chairman of the Small Agency Council is responsible for, on an ongoing basis, in coordination with the Secretary of Homeland Security, providing a forum for development and integration of continuity policies and programs among the Federal Government organizations represented on the Council.
- n. FEBs and FEAs are responsible for, on an ongoing basis, providing assistance where practicable in coordinating continuity activities for FEB and FEA members.
- o. Federal Intelligence and Law Enforcement Communities are responsible for providing intelligence through existing channels to NFGs as appropriate, using official processes and communications methods.
- p. Department and Agency Continuity Coordinators are responsible for:
- 1) Ensuring effectiveness and survivability of the organization's continuity capability.
 - 2) Representing their organization and offering practical recommendations on continuity policy.
 - 3) Representing their agency on the CAG or designating a representative to attend in their place.
 - 4) Working with their agency heads to complete the MEF and PMEF identification process.
 - 5) Ensuring that Continuity Managers and Planners are provided the authority and are positioned at a level to effectively oversee the day-to-day management of their continuity program.
 - 6) As required, ensuring that Continuity Readiness Reports, and other reports as requested, are submitted through the RRS.
- q. Continuity Managers and Planners are responsible for:
- 1) Managing day-to-day continuity programs.
 - 2) Representing their agency on the CAG and working groups, as appropriate.
 - 3) Reporting to the Continuity Coordinator, as appropriate.
 - 4) Working with their agencies' heads and in conjunction with their agencies' Continuity Coordinators to complete the process of MEF and PMEF identification.
 - 5) Fully understanding their organizations and monitoring the direction, guidance, and best practices of both the government and the private sector to develop the most relevant and robust continuity programs.
 - 6) Ensuring that the Continuity Coordinator is apprised of the overall status of the continuity program.
 - 7) Providing other support to the Continuity Coordinator as directed.
-

- r. Individuals are responsible for:
- 1) Understanding their continuity roles and responsibilities within their respective organizations.
 - 2) Knowing and being committed to their duties in a continuity environment.
 - 3) Understanding and being willing to perform in continuity situations to ensure an organization can continue its essential functions.
 - 4) Ensuring that family members are prepared for and taken care of in an emergency situation.

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 FEMA, National Continuity Programs Directorate, at 202.646.4145.

14. DISTRIBUTION: This FCD is distributed to the heads of Federal agencies, senior policy officials, emergency planners, and other interested parties.

ANNEX A. PROGRAM PLANS AND PROCEDURES

An effective continuity program is implemented through its related continuity plans and procedures and an effective continuity test, training, exercise, and operational capability to support those plans and procedures. An essential part of developing a comprehensive continuity plan is the establishment of planning and procedural objectives and requirements. Metrics shall be used to measure an agency's ability to meet its continuity requirements.

PLANNING OBJECTIVES: Continuity planning is an effort to document and ensure the capability of continuing agency essential functions during a wide range of potential emergencies. The objectives of a continuity plan include:

1. Ensuring that an agency can perform its Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs), if applicable, 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 agency's leadership unavailable, or incapable of assuming and performing their authorities and responsibilities of office.
4. Reducing or mitigating disruptions to operations.
5. Ensuring that the agency has facilities where it can continue to perform its MEFs and PMEFS, as appropriate, during a continuity event.
6. Protecting personnel, essential facilities, equipment, records, and other assets, in the event of a disruption.
7. Achieving the agency's timely and orderly recovery and reconstitution from an emergency.
8. Ensuring and validating continuity readiness through a dynamic and integrated continuity test, training, and exercise (TT&E) program and operational capability.

REQUIREMENTS FOR CONTINUITY PLANS AND PROCEDURES: Agencies shall develop and maintain continuity plans and procedures that, when implemented, provide for the continued performance of their essential functions under all circumstances, and the integration with other government and non-government organizations as appropriate. Each individual agency's continuity program should be tailored to ensure that organization's MEFs and PMEFS, as appropriate, can be performed under all conditions.

Risk management principles shall be applied to all elements of continuity planning. Risk management is the process to identify, control, and minimize the impact of uncertain events. Although there are many well-documented methodologies for risk management—some of these are referred to as risk analysis—most require an assessment and understanding of three basic concepts:

- The consequences of not protecting valuable assets (i.e., people, information, and facilities) and/or not performing essential functions.
- The threat environment (as it relates to a particular agency or area of concern).
- The level of vulnerability to the relevant threats.

Reviewing an organization's risks and risk management programs must take into consideration additional factors such as the probabilities of events occurring, mission priorities, and impact assessments. Further, cost may also be a factor to consider, 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. Risk can never be fully mitigated, 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 to apply funding and other assets.

A continuity threat assessment integrates a historical review of past events that have affected normal operations (e.g., natural disasters; disruptions of communication, power, and other utilities; threats to public safety) with a dynamic analysis of other potential forms and likelihoods of threats, such as acts of terrorism (from both foreign and domestic agents) and war.

As an integral part of risk management, an organization's leaders must think beyond the internal effects of their inability to perform PMEFs and MEFs. Agency heads and staff at all levels must also consider the interdependencies between and among agencies that share critical roles in the delivery of National Essential Function (NEF) capabilities. To the extent possible, agencies should partner with State, local, territorial, and tribal governments, as well as with owners and operators of private-sector critical infrastructure and key resources (CI/KR), to develop continuity plans that are consistent with the Federal Government's plans.

A continuity plan and its supporting procedures shall be developed and documented so that, when implemented, the plan and procedures will provide for the continued performance of an organization's essential functions under all circumstances. The continuity plan must do the following:

1. Identify MEF's and PMEF's, if applicable.
2. Address the key elements of continuity: essential functions, orders of succession, delegations of authority, alternate facilities, interoperable communications, vital records, human capital, TT&E, devolution, and reconstitution.
3. Establish, for the position of organizational head as well as for supporting key positions, orders of succession and preplanned delegations of authority, to ensure there is an orderly and predefined transition of leadership and delegation of authority within an agency during any emergency. Succession orders and delegations of authority must be planned and documented in advance and in accordance with applicable laws, to ensure the performance of an agency's MEFs and PMEFs.
4. Identify and establish procedures to ensure vital resources, facilities, and records are safeguarded, available, and accessible to support continuity operations. Vital resources should include personnel, equipment, systems, infrastructures, supplies, and other assets required to perform an agency's MEFs and PMEFs.
5. Identify provisions for the acquisition of necessary personnel and resources for continuity operations on an emergency basis. These provisions must be available for up to 30 days or until normal operations can be resumed.

6. Identify and provide for the availability and redundancy of critical communications capabilities at primary sites, alternate sites, in transit, and other continuity sites including telework sites, as appropriate, to ensure the performance of the agency's MEFs and PMEFS and to support connectivity between and among key government leaders, internal elements, other executive agencies, critical partners, and the public. Category I and select Category II agencies shall coordinate with the Secretary of Homeland Security and the Secretary of Defense to obtain and operate secure and integrated Continuity of Government (COG) communications. Classified information should be documented in classified annexes to relevant continuity and communications plans.
7. Provide the ability to recover from the effects of an emergency and reconstitute operations and resources, so that the agency can return to a fully operational condition in the aftermath of an incident. Agencies shall coordinate and plan as necessary to ensure a return to normal operations.
8. Identify the components, processes, and requirements for the identification, training, and preparedness of personnel who are capable of relocating to alternate facilities to support the continuation of the performance of MEFs and PMEFS.
9. Identify the components, processes, and requirements that ensure the continued performance of an agency's MEFs and PMEFS.
10. Outline a process for determining the agency's readiness posture and for decisionmaking regarding its corresponding actions to implement continuity plans and procedures.
11. Establish alert and notification procedures for all continuity personnel throughout all phases of a continuity event, including processes for monitoring the Department of Homeland Security's (DHS) Homeland Security Advisory System (HSAS), the Federal Government Response Stages for Pandemic Influenza, intelligence, and other advisory information. Establish internal procedures for executing changes to the Continuity of Government Readiness Conditions (COGCON), as appropriate. These procedures should also consider regional, State, territorial, tribal governments' or private sector continuity preparedness or activation directions. Establish a process for reporting continuity readiness and activation status in accordance with guidance provided in Annex M, Reconstitution Operations, and Annex N, Continuity Plan Operational Phases and Implementation.
12. Define the roles and responsibilities of those individuals who support the agency's continuity program.
13. Establish and maintain appropriate point of contact (POC) rosters of trained continuity personnel who are fully equipped and who have the authority to perform essential functions, including the execution of the devolution of control plan.
14. Establish and maintain the appropriate relocation procedures and guidance for continuity personnel.
15. Provide the ability to communicate with and coordinate activities with non-continuity personnel.
16. Ensure that the continuity plan can be implemented both with and without warning.
17. Ensure that in all cases, PMEFS will be either performed continuously during the course of an event or resumed within 12 hours of an event.

18. Ensure that the continuity plan can become operational within the minimal acceptable period for MEF disruption, but in all cases within 12 hours of plan activation.
19. Ensure that sustained operations can be maintained for up to 30 days after an event or until normal business activities can be resumed. This includes planning for the challenges posed by extended events (like a pandemic) that occur in repeated waves.
20. Ensure there is a provision for an all-hazards risk assessment of all agency continuity facilities.
21. Identify and prepare all agency continuity facilities.
22. Recommend content and maintenance of drive-away kits.
23. Establish contingency plans for the performance of PMEFS and MEFs in the event key resources, including Emergency Operating Records, supplies, and personnel, are not available.
24. Include provisions and procedures for assisting all agency staff, especially those who are disaster victims, with special human capital concerns following a catastrophic disaster.
25. Provide guidance to all staff in developing Family Support Plans which will increase personal and family preparedness throughout the organization.

CONTINUITY REQUIREMENTS AND METRICS: From the list of continuity requirements (see below), agency heads shall use the key questions and metrics guidance below to annually certify to the NCC that their organizations have a robust continuity capability.

NSPD-51/HSPD-20 Paragraph 11 – Continuity requirements for the Executive Office of the President (EOP) and executive branch departments and agencies shall include the following:			
	CONTINUITY REQUIREMENTS	KEY QUESTIONS	METRICS <i>(Provide justification including quantitative and/or qualitative data to show you have met the requirement <OR> identify steps you will take to do so.)</i>
1.	The continuation of the performance of PMEFS during any emergency must be for a period up to 30 days or until normal operations can be resumed, and the capability to be fully operational at alternate sites as soon as possible after the occurrence of an emergency, but not later than 12 hours after COOP activation;	<ul style="list-style-type: none"> • Is your organization able to perform your current PMEFS during any emergency and for up to 30 days or resumption of normal operations? • Is your organization able to be fully operational at an alternate site within 12 hours of COOP activation? 	<ul style="list-style-type: none"> • Measure ability to perform PMEFS through test, training, and exercise, identifying gaps and solutions. • Measure capability to be fully operational at a COOP site within 12 hours through test, training, and exercise, identifying gaps and solutions.
2.	Succession orders and pre-planned devolution of authorities that ensure the emergency delegation of authority must be planned and documented in advance in accordance with applicable law;	<ul style="list-style-type: none"> • Does your organization have accessible and complete orders of succession familiar to successors? • Does your organization have accessible and complete devolution of authorities known by those to whom they devolve? 	<ul style="list-style-type: none"> • Document and train on succession orders • Document and train on devolution of authorities
3.	Vital resources, facilities, and records must be safeguarded, and official access to them must be provided;	<ul style="list-style-type: none"> • Are your vital resources safeguarded? • Are your facilities safeguarded? • Are your records safeguarded? • Will your continuity staff have official access to your vital resources, facilities, and records in an emergency? 	<ul style="list-style-type: none"> • Document measures taken to safeguard vital resources, facilities, and records. • Document measures taken to ensure official access to vital resources, facilities, and records.

	CONTINUITY REQUIREMENTS	KEY QUESTIONS	METRICS <i>(Provide justification including quantitative and/or qualitative data to show you have met the requirement <OR> identify steps you will take to do so.)</i>
4.	Provision must be made for the acquisition of the resources necessary for continuity operations on an emergency basis;	<ul style="list-style-type: none"> • Have you identified emergency continuity resources? • Do you have agreements/ contracts to acquire emergency continuity resources? 	<ul style="list-style-type: none"> • Identify your emergency continuity resource requirements. • Identify what agreements/ contracts you have made to meet these requirements. • Identify what additional agreements/contracts are needed.
5.	Provision must be made for the availability and redundancy of critical communications capabilities at alternate sites in order to support connectivity between and among key government leadership, internal elements, other executive departments and agencies, critical partners, and the public;	<ul style="list-style-type: none"> • Do you have critical communications capability at your alternate site(s)? • Do you have redundant communications capability at your alternate site(s)? 	<ul style="list-style-type: none"> • Identify your current communications capability at your alternate site. • Identify what communications capability is necessary • Identify the plan to improve communications at your alternate site in six months, one year, and two years.
6.	Provision must be made for reconstitution capabilities that allow for recovery from a catastrophic emergency and resumption of normal operations; and	<ul style="list-style-type: none"> • What is your plan to ensuring your reconstitution capability? 	<ul style="list-style-type: none"> • Identify your reconstitution capability plan.
7.	Provision must be made for the identification, training, and preparedness of personnel capable of relocating to alternate facilities to support the continuation of the performance of PMEFs.	<ul style="list-style-type: none"> • Have you identified, trained, and prepared personnel to relocate to alternate sites to continue PMEFs? 	<ul style="list-style-type: none"> • Verify that staff are identified, trained, and prepared to relocate to alternate sites.

Table 1: Continuity Requirements and Metrics

For each of the seven continuity requirements, agency heads will self-identify a simple grading system, consistent with the President’s Management Agenda to show status:

- Green for success,
- Yellow for mixed results, and
- Red for unsatisfactory.

ANNEX B. RISK MANAGEMENT

Risk management is a process to identify, control, and minimize the impact of uncertain events. This process supports the overarching Continuity Program Management Cycle by identifying (1) the critical risks to organizational readiness and (2) the strategies that best mitigate the risks.

The recommended risk management cycle is made up of five analytical and management phases (see Figure 4): (1) setting strategic goals and objectives, and determining constraints; (2) assessing the risks; (3) evaluating alternatives for addressing these risks; (4) selecting the appropriate alternatives; and (5) implementing the alternatives and monitoring the progress made and the results achieved. This cycle was introduced by the Government Accountability Office (GAO)¹ in 2005. The GAO risk management cycle, while generic, provides a useful framework for maximizing the readiness of an organization to perform its Primary Mission Essential Functions (PMEFs) and Mission Essential Functions (MEFs) in the face of risks from a broad spectrum of hazards facing the organization, both manmade and natural. This process organizes information about the possibility of a spectrum of unwanted outcomes into an inclusive, orderly structure that helps decision makers make more informed choices about risks to the organization's readiness across the four pillars that comprise the Nation's continuity capability: leadership, staff, facilities, and communications. The continuity requirements detailed in National Security Presidential Directive (NSPD)-51/ Homeland Security Presidential Directive (HSPD)-20 Paragraph 11 provide a set of key questions and metrics to help guide the risk management process.



Figure 4

The following sections describe the key elements that an organization's analysis team must address in each of the phases of the risk management cycle.

Phase 1 – Strategic Goals, Objectives, and Constraints

This phase involves establishing the scope and structure of the risk-informed decision making process. Critical steps in this phase include:

- **Understand and define the decision.** For this effort, the critical question is: *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?*
- **Determine who should be involved.** Input from key stakeholders is essential to a sound risk management process. The analysis team should identify and solicit input from

¹ Government Accountability Office; Protection of Chemical and Water Infrastructure Federal Requirements, Actions of Selected Facilities, and Remaining Challenges, March 2005, GAO-05-327

stakeholders who should be involved in making the decision, and those who will be affected by actions resulting from the decision making process.

- **Identify the factors that will influence the decisions.** The decision to invest resources to meet continuity requirements is not based on only one factor. Decision makers must simultaneously weigh multiple factors, including costs, timelines, and risks.

Phase 2 – Risk Assessment

This phase involves following a structured process for understanding the problem facing an organization. Simply, this process provides this understanding by answering the following three questions: (1) what can go wrong, (2) what is the likelihood that the undesired event might occur, and (3) what would be the impact should it occur? Critical steps in this phase include:

- **Inventory the critical functions provided by the organization.** The analysis team should leverage the functions identified during the PMEF Identification and Analysis process (see Annex D).
- **Identify the hazards that can impact delivery of the critical functions.** This step would include exploring potential natural events, intentional man-made events, and non-intentional man-made events that could adversely affect the ability of the organization to perform PMEFs. Natural hazards are those where the occurrence is beyond the control of the organization, including earthquakes, floods, ice storms, winter weather, and external fires. Intentional man-made hazards are also beyond the direct control of the organization and could include events such as external sabotage, and terrorism. Non-intentional man-made events, such as power outages, fires, explosions, equipment failures, or human errors are generally within the control of the organization.
- **Develop continuity hazard scenarios.** All of the assessment steps should be performed within the context of a set of scenarios, each of which is a unique combination of a particular hazard and the organization's PMEF. Within each scenario, the analysis team should consider risks to all four continuity pillars, as appropriate, recognizing that in most cases, all of the pillars must be available in order to deliver the function. The following steps outline the elements of the scenario risk assessment:
 - **Determine the risk information needed to assess the risk.** Describe the information necessary to assess the risk for each scenario. For each information item, specify the information type, precision, and certainty required, and the analysis resources available.
 - **Assess the risk.** For each scenario, the analysis team should assess the threat, vulnerability, and consequence, where:
 - *Threat* is the likelihood of a type of attack that might be attempted, or that the scenario will occur.
 - *Vulnerability* is the likelihood that an attacker would succeed with a particular attack type, or that the scenario will result in the expected level of consequence.
 - *Consequence* is the potential impact of a particular attack, or the negative impact of the scenario.

For this effort, consequence should be expressed in terms of failure to deliver the National Essential Functions (NEFs) (see Annex D). When evaluating consequences, the analysis team should consider both short- and long-term

impacts for disasters and accidents as well as intended and unintended effects from intentional attacks.

Depending on the nature of the scenario, the analysis team can use different tools to assess the scenario's risk. For instance, the team may be able to leverage historical accident reporting databases to assess the risk of accident scenarios; while detailed stochastic models may be available for assessing the risk of natural hazard scenarios. For scenarios where historical data or detailed modeling are scarce, subject matter expertise must be leveraged to produce the risk assessment.

- **Identify existing safeguards/countermeasures.** For each scenario, the analysis team should identify the existing safeguards that are in place to reduce either the likelihood (e.g., security countermeasures) or consequence (e.g., redundant capabilities) of the hazard.

Phase 3 – Evaluation of Alternates

For many scenarios, the current risk may be considered to be at an acceptable level. For those scenarios where the current level of risk is deemed to be unacceptable, action(s) must be taken to mitigate the risk. These actions must (1) provide a beneficial return on investment, (2) be acceptable to stakeholders, and (3) not cause other significant risk. Critical steps in this phase include:

- **Develop alternate risk management strategies.** The analysis team should engage the appropriate stakeholders to determine how the risks for each scenario can be managed most effectively. These alternate strategies should be completely developed and documented by addressing all of the critical factors (e.g., cost, schedule).
- **Assess the risk impact of the proposed strategies.** The analysis team should reassess the risk of each scenario based on the implementation of each alternative strategy. This step will provide the risk reduction value of each of the alternate strategies.

Phase 4 – Management Selection

Once the alternative strategies have been fully developed and their risk reduction value has been quantified, the risk management process moves to the management selection phase, where decision makers choose the collection of alternatives for implementation. The alternatives will be evaluated based on consideration of all of the previously identified critical factors, including effectiveness (risk reduction), efficiency, and cost-effectiveness.

Another critical factor that should be considered is the confidence or belief that the alternative will achieve the projected level of performance. The effect of many of the alternative strategies may be well understood by the organization. For instance, these alternatives may have a proven track record of performance within other similar organizations, or they may have been extensively studied. The performance of other alternatives with less of a history may not be as well understood. The analysis team may believe that these less understood alternatives will achieve a level of satisfactory performance; however, their confidence is at a lower level.

During the management selection phase, decision makers need an understanding of both anticipated performance and confidence to ensure that the proper suite of actions is taken. Figure 5 represents a simple decision support matrix that recommends approaches for dealing with different levels of anticipated performance and confidence.

Finally, decision makers must recognize that this process is cyclical and many of the alternatives will be implemented in subsequent cycles due to limitations in resources and time.

Anticipated Performance	Satisfactory (near or above goal)	<ul style="list-style-type: none"> • Work to improve confidence AND • Investigate other strategies 	<ul style="list-style-type: none"> • Maintain current strategy OR • Move to strategy with better anticipated performance and confidence
	Unsatisfactory (below goal)	<ul style="list-style-type: none"> • Work to improve confidence AND • Aggressively prepare to select another strategy 	<ul style="list-style-type: none"> • Change implementation of current strategy OR • Implement new strategy
		Unsatisfactory (Low)	Satisfactory (High)

Confidence

Figure 5

Phase 5 – Implementation & Monitoring

Critical steps in this phase include:

- **Implement the chosen mitigation strategies.** This step involves the implementation of the mitigation strategies identified during the management selection phase. These strategies should reduce the risk that the organization will be unable to meet the continuity requirements.
- **Develop metrics to measure effectiveness.** The analysis team must develop a collection of metrics, both qualitative and quantitative, to measure the organization’s ability to meet the continuity requirements. The metrics identified in NSPD-51/HSPD-20 Paragraph 11 for each of the continuity requirements should serve as a guide in crafting the metrics.
- **Monitor organizational performance.** After the strategies have been implemented and the metrics have been developed, the organization should monitor the effectiveness of the actions taken to manage risk. The goal of the monitoring phase is to verify that the organization is getting the expected results from its risk management decisions. Key inputs into the monitoring phase include testing, training, and exercising. The results of the monitoring step will inform subsequent iterations of the risk management cycle.

Summary

The risk management cycle involves a series of basic steps that can be performed at different levels of detail with varying degrees of formality, depending on the situation. The key to using this process is completing each step in the most simple, practical way to provide information to the decision maker.

ANNEX C. BUDGETING AND ACQUISITION OF RESOURCES

Agencies must identify the people, communications, facilities, infrastructure, and transportation requirements, which are necessary to the successful implementation and management of an agency'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 agency's leaders and staff will ensure critical continuity resources are available to continue performing the agency's essential functions before, during, and after a continuity event.

As directed in National Security Presidential Directive (NSPD)-51/ Homeland Security Presidential Directive (HSPD)-20 and in the National Continuity Policy Implementation Plan, all agencies must identify and provide continuity funding and specific budgetary requirements for all levels of their organizations, including subordinate components and regional- and field-level offices. These budgetary procedures and requirements will directly support and enable agencies' ability to meet the criteria outlined in this Federal Continuity Directive (FCD) for a viable continuity capability.

The Director of the Office of Management and Budget (OMB) reviews all funding requests for continuity activities and evaluates department and agency performance in executing continuity budgets. The Director, in coordination with the National Continuity Coordinator (NCC), issues guidance to assist departments and agencies with continuity budget submissions.

Actions according to the Implementation Plan for the Director of the Office of Management and Budget (OMB)

1. As necessary, in coordination with the NCC, issue continuity planning guidance for the development of continuity budget requests.
2. Annually conduct an assessment of agency continuity funding requests and performance data that are submitted by executive branch agencies as part of the annual budget request process in order to monitor progress in the execution of the *Plan* and continuity budgets.
3. Annually reconcile agency continuity funding requests and performance data with Continuity Readiness Reporting and annual continuity assessments compiled by the Federal Emergency Management Agency (FEMA).

To ensure effective continuity capabilities, the agency must

1. Use a risk management methodology to identify, prioritize, and justify the allocation of continuity budgetary resources.
2. Integrate continuity budgets with a multiyear strategy and a program management plan, and link the budgets directly to objectives and metrics set forth in that plan.
3. Provide for the acquisition of those resources necessary for continuity operations on an emergency basis.
4. Budget for and acquire continuity capabilities in accordance with NSPD-51/HSPD-20 and the National Communications System's (NCS) Directive 3-10 (continuity communications), as applicable.

Budget and Acquisitions Considerations

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

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

Further, cost may also be a consideration, 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.

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 and services will remain uninterrupted across a wide range of potential emergencies and provides a mechanism for the resumption of all functions as resources become available.

All agencies must identify and prioritize their essential functions as the foundation for continuity planning. Essential functions, broadly speaking, are those functions that enable an organization to provide vital services, exercise civil authority, maintain the safety of the general public, and sustain the industrial/economic base during an emergency. The goal of this annex is to assist with the identification, prioritization, and resourcing of these essential functions.

This annex is divided into two sections. The first, Mission Essential Functions (MEFs), addresses the identification of government functions and fundamental continuity planning based on the determination of which of these is considered a MEF, and their individual priority in the overall mission of an agency. The second, Primary Mission Essential Functions (PMEFs), addresses the connection between an agency's MEFs and the National Essential Functions (NEFs), which ensure continuity at the highest levels of government.

SECTION 1: MEFs

Agencies at every level of government provide a broad cross-section of government functions. The task of separating MEFs from those government functions is an early and critical component of continuity planning. Preparing a list of all the government functions performed by an agency is a prerequisite to identifying those specific actions which must be performed in order to implement one or more essential functions. The process used to identify organizational functions may vary, depending on the mission and structure of an organization.

The identification of government functions will focus on defining the activities an agency conducts to accomplish its mission and serve its stakeholders. It is critical to recognize the difference between government functions and the tasks that support them. While these tasks should not be included on the list of government functions, it is important to identify them for ensuring the capability to implement both government functions and essential functions. Identification of these government functions and supporting tasks will be beneficial in implementing continuity programs and reconstitution plans after an event.

An agency should carefully review all of its missions and functions before determining those that are essential. Improperly identifying functions as "essential" or not identifying as "essential" those functions that are, can impair the effectiveness of the entire continuity program, because other aspects of the plan are designed around supporting these functions. If an agency fails to identify a function as essential, that agency will not identify the requirements and resources to support that function in an emergency and will not make the necessary arrangements and coordination to perform that function. If an agency identifies too many functions as essential, the agency risks being unable to adequately address all of them. In either case, the agency

increases the risk that it will not be able to perform all of its essential functions during a continuity event.

Planning related to essential functions must also include identifying those agency partners who are critical to program delivery, testing the effectiveness of data exchange among the organization's partners, developing complementary continuity plans with those partners, sharing key information on readiness with partners and the public, and taking steps to ensure that the performance of the agency's essential functions will be sustained during a continuity event. There must be careful consideration of agency and other partner interdependencies, to ensure the continued delivery and performance of essential functions across a full spectrum of threats and all-hazards emergencies.

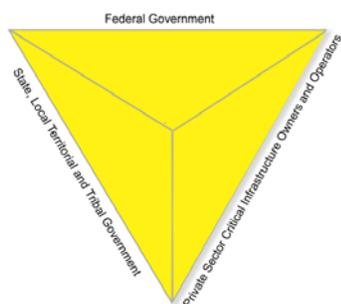


Figure 6

While this Directive is primarily directed at the executive branch of the Federal Government, continuity cannot occur without the commitment and dedication of many partners who play integral roles in ensuring homeland security and providing critical functions and services to the Nation's citizens.

These partners include the following (see Figure 6):

- Federal Government: legislative branch, executive branch (including all departments and agencies), and judicial branch;
- State, local, territorial, and tribal governments; and
- Private sector critical infrastructure owners and operators.

To support its continuity requirements, the Federal executive branch prioritizes the following three categories of essential functions:

- Mission Essential Functions (MEFs): The limited set of agency-level government functions that must be continued after a disruption of normal activities.
- Primary Mission Essential Functions (PMEFs): A subset of agency MEFs that directly support the National Essential Functions.
- National Essential Functions (NEFs): The eight functions the President and national leadership will focus on to lead and sustain the Nation during a catastrophic emergency.

The following relationship between government functions and Mission Essential Functions is illustrated in Figures 7 and 8.

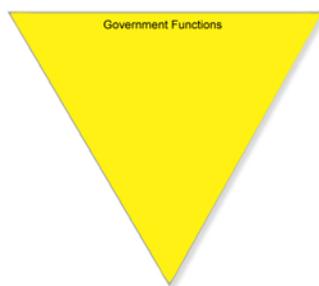


Figure 7

Government functions (see Figure 7) are the collective functions of agencies, as defined by the Constitution, statute, regulation, presidential direction, or other legal authorities, and the functions of the legislative and judicial branches. The activities of State, local, territorial, and tribal governments and private sector organizations often support Federal Government functions, particularly in the protection of critical infrastructure and key resources (CI/KR). These interdependencies rely upon a greater interoperability between and among these partners, to facilitate a more rapid and effective response to and recovery from any emergency.

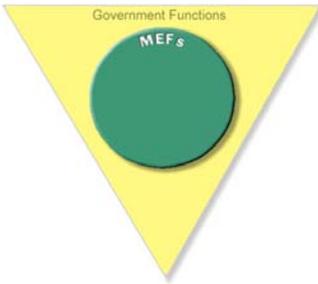


Figure 8

MEFs are described as the limited set of agency-level government functions (as depicted in Figure 8) that must be continued throughout, or resumed rapidly after, a disruption of normal activities. 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 and economic base, during the disruption of normal operations. Once identified, MEFs serve as key continuity planning factors for agencies to determine appropriate staffing, communications, information, facilities, training, and other continuity requirements.

Process – MEF Identification and Analysis

Identifying department and agency MEFs is a prerequisite for continuity because it establishes the parameters that drive the department and agency efforts in all other planning and preparedness areas. For a government function to be identified as a MEF, the National Continuity Policy Implementation Plan provides the following guidance (see Figure 9).

MEF Initial Screening Aid		
Is the function directed by law, presidential directive, or executive order? If yes, identify which:	YES	NO
Did a Business Process Analysis (BPA) determine that the function must be performed under all circumstances either uninterrupted, with minimal interruption, or requiring immediate execution in an emergency?	YES	NO
<i>If the answer to one or both of these questions is "No," the function is probably not a MEF.</i>		

Figure 9

Agencies will do the following when identifying and analyzing MEFs (see Figure 10):

- Review their organization’s functions as directed by applicable law, presidential directives, executive orders, or other executive branch directives, to identify their MEFs.
- Conduct a MEF BPA to identify and map the functional processes, workflows, activities, personnel expertise, systems, data, and facilities inherent to the execution of each identified MEF (e.g., define how each MEF is performed and executed, using a business-process flow map) that must be performed under all circumstances either uninterrupted, with minimal interruption, or requiring immediate execution in an emergency.
- Identify those MEFs that provide vital interdependent support to a MEF performed by another agency or by an Emergency Support Function (ESF) under the National Response Framework (NRF).
- Identify those MEFs that require vital support from another agency to ensure the execution of their mission and identify when and where the particular interdependency is executed within the BPA business-process flow.
- Validate and approve the identified MEFs and BPA analysis by each agency head.

PROCESS FOR MEF IDENTIFICATION

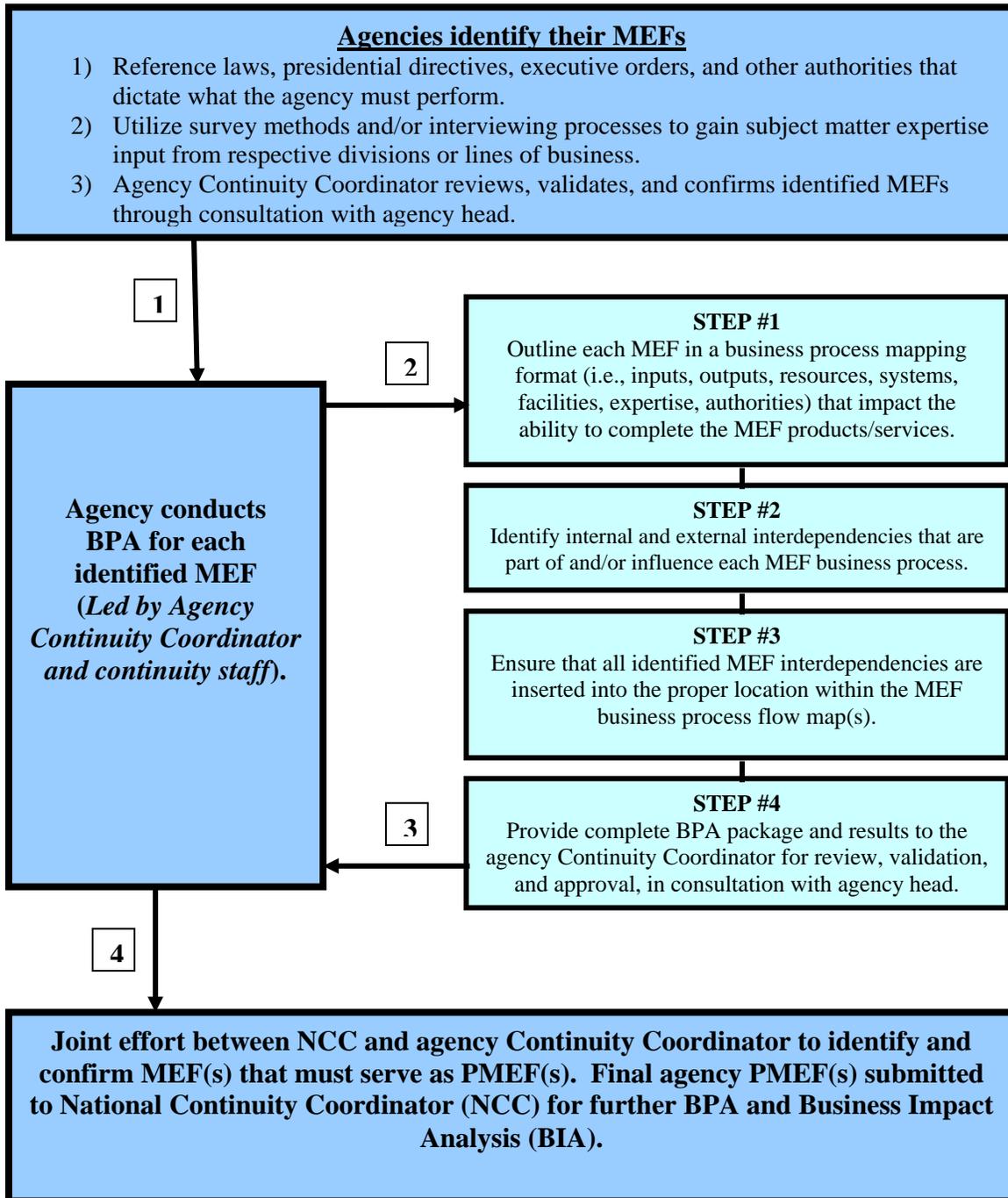


Figure 10

SECTION 2: PMEFs

Once MEFs have been identified and analyzed, the planning process for identifying the PMEFs can begin. Directly linking PMEFs to an NEF requires Federal executive agencies to identify the most critical functions that must continue during an emergency, as well as the planning required to perform those functions. This model may serve as a template for other government organizations and for private sector entities.

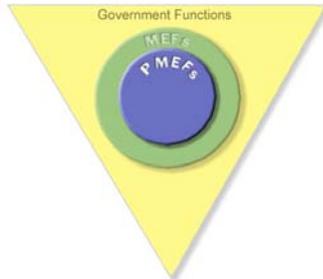


Figure 11

PMEFs are those agency Mission Essential Functions, validated by the NCC, which must be performed in order to support the performance of the NEFs before, during, and in the aftermath of an emergency (see Figure 11). PMEFs are defined as those functions that 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.

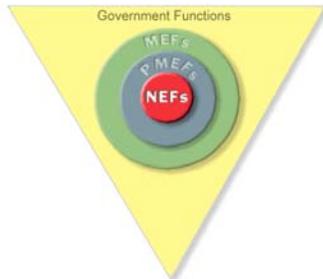


Figure 12

In accordance with National Security Presidential Directive (NSPD)-51/ Homeland Security Presidential Directive (HSPD)-20, the eight NEFs represent the overarching responsibilities of the Federal Government to lead and sustain the Nation and shall be the primary focus of the Federal Government's leadership during and in the aftermath of an emergency (see Figure 12).

Figure 13 shows the interdependencies of the key partners and the functions of continuity. Independent government entities at all levels and individual private sector companies are intimately connected and work together in critical partnership to ensure continuation of essential functions.

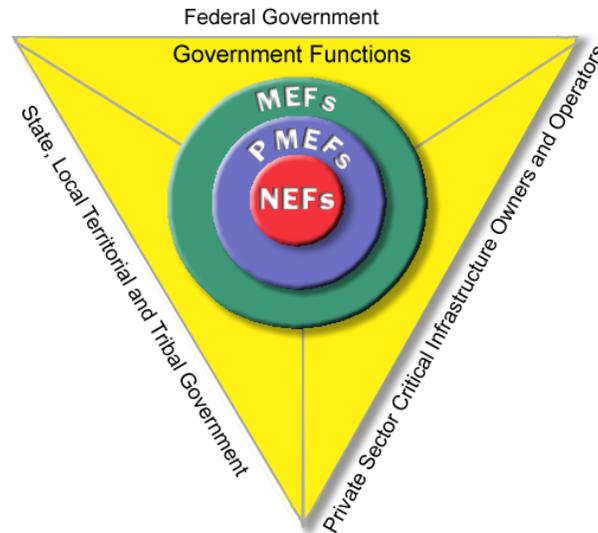


Figure 13

NEFs

The eight NEFs are the foundation for all continuity programs and capabilities and represent the overarching responsibilities of the Federal Government to lead and sustain the Nation during a crisis, and therefore sustaining the following NEFs shall be the primary focus of the Federal Government leadership during and in the aftermath of an emergency that adversely affects the performance of government functions. These are categories of functions performed by one or more agencies; they are not new authorities, requirements, or functions.

1. Ensuring the continued functioning of our form of government under the Constitution, including the functioning of the three separate branches of government. This NEF includes Federal executive branch functions that respect the roles and maintain the check and balance relationship among all three branches of the Federal Government.
2. Providing leadership visible to the Nation and the world, and maintaining the trust and confidence of the American people. This NEF includes Federal executive department and agency functions to demonstrate that the Federal Government is viable, functioning, and effectively addressing any emergency.
3. Defending the Constitution of the United States against all enemies, foreign and domestic, and preventing or interdicting attacks against the United States or its people, property, or interests. This NEF includes Federal executive department and agency functions to protect and defend the worldwide interests of the United States against foreign or domestic enemies, honor security agreements and treaties with allies, implement military operations ordered by the President, maintain military readiness, and maintain preparedness to achieve national objectives.

4. Maintaining and fostering effective relationships with foreign nations. This NEF includes Federal executive department and agency functions to maintain American foreign policy.
5. Protecting against threats to the homeland and bringing to justice perpetrators of crimes or attacks against the United States or its people, property or interests. This NEF includes Federal executive department and agency functions to protect against, prevent, or interdict attacks on the people or interests of the Nation and to identify, neutralize, and prosecute those who have committed or intend to commit violations of the law.
6. Providing rapid and effective responses to and recovery from the domestic consequences of an attack or other incident. This NEF includes Federal executive department and agency functions to implement response and recovery plans, including, but not limited to, the implementation of the National Response Plan.
7. Protecting and stabilizing the Nation’s economy and ensuring public confidence in its financial systems. This NEF includes Federal executive department and agency functions to respond to and recover from the economic consequences of an attack or other major impact on national or international economic functions or activities.
8. Providing for critical Federal Government services that address the national health, safety, and welfare needs of the United States. This NEF includes Federal executive department and agency functions that ensure that the critical Federal-level health, safety, and welfare services of the Nation are provided during an emergency.

Process – PMEF Identification and Analysis

PMEF Initial Screening Aid		
Does the function directly support a NEF? If yes, identify which: 1 2 3 4 5 6 7 8	YES	NO
Does the function need to be continued uninterrupted or need to be resumed within 12 hours, regardless of circumstance?	YES	NO
<i>The answers to both of these must be “YES” for the function to be considered a PMEF.</i>		

Figure 14

PMEF identification is an iterative process performed by each department and agency in coordination with the NCC. In order to identify and analyze PMEFs, the following actions will take place (see Figure 15):

- Upon MEF approval by each department or agency head, a joint effort between the NCC and each department or agency Continuity Coordinator and staff will result in a preliminary identification of PMEFs that potentially support NEFs. The joint effort will culminate in the department or agency’s submission of PMEF identification results to the NCC for further interagency analysis.

- An interagency board (IAB), established by the NCC, conducts a review of submitted potential PMEFS and validates the PMEFS' relationship to the NEFS. A BIA will be used to ensure that the PMEFS are appropriate and relevant.
- Upon confirmation that the IAB has determined that a department or agency's MEF shall serve as a PMEFS, each department and agency will revisit the prioritization of their MEF recovery timelines to ensure PMEFS' criticality.
- The IAB will conduct a BPA to identify and map interagency PMEFS processes, workflows, activities, expertise, systems, data, and facilities inherent to the interagency execution of each NEF. The BPA should also define the PMEFS' relationship to the NEF. In other words, the BPA will define how each NEF is executed via business process flow mapping (i.e., NEF serving as the "end product output" and interagency PMEFS serving as the functional "inputs").
- The IAB must also conduct an analysis of interagency PMEFS interdependencies within each NEF to accurately depict each department or agency's PMEFS execution capability and dependencies. The IAB will conduct NEF-specific BIAs to: (1) identify potential single points of failure that may adversely affect the execution of the interagency PMEFS support to NEFS; (2) define the impact of downtime (i.e., impact of delayed PMEFS recovery on NEF execution); and (3) define potential PMEFS process alternatives/work-around solutions.
- The NEF BPAs, BIAs, and the interagency list of PMEFS are submitted to the NCC for final approval.

The immediacy of maintaining or recovering essential functions capability is driven by the results of the MEF and NEF BPAs and the NEF BIAs. Subsequently, the described risk management approach requires an emphasis on the geographic dispersion, redundancy, and survivability of leadership, staff, and infrastructure. Planners should assume that they will have no warning of the threats that we face in today's world. Threats might come from known or unknown sources. The nature of asymmetric threats is that they do not necessarily emanate from a single, fixed, and understood actor; asymmetric threats are, in many ways, less predictable and less understood, requiring planners to consider different approaches to plan for, mitigate, and respond to threats.

A successful BPA will identify gaps within a department or agency and areas where more than one department or agency has responsibilities. This gap identification provides departments and agencies an opportunity to fill the gap and ensure successful execution of essential functions and preparation for incident management. While the Department of Homeland Security (DHS) has primary incident management responsibility, many different departments and agencies at multiple levels are involved in successfully navigating a critical incident management scenario.

Continuity requirements must be incorporated into the daily operations of all executive branch agencies to ensure seamless and immediate continuation of PMEFS capabilities.

PROCESS FOR PMEUF IDENTIFICATION

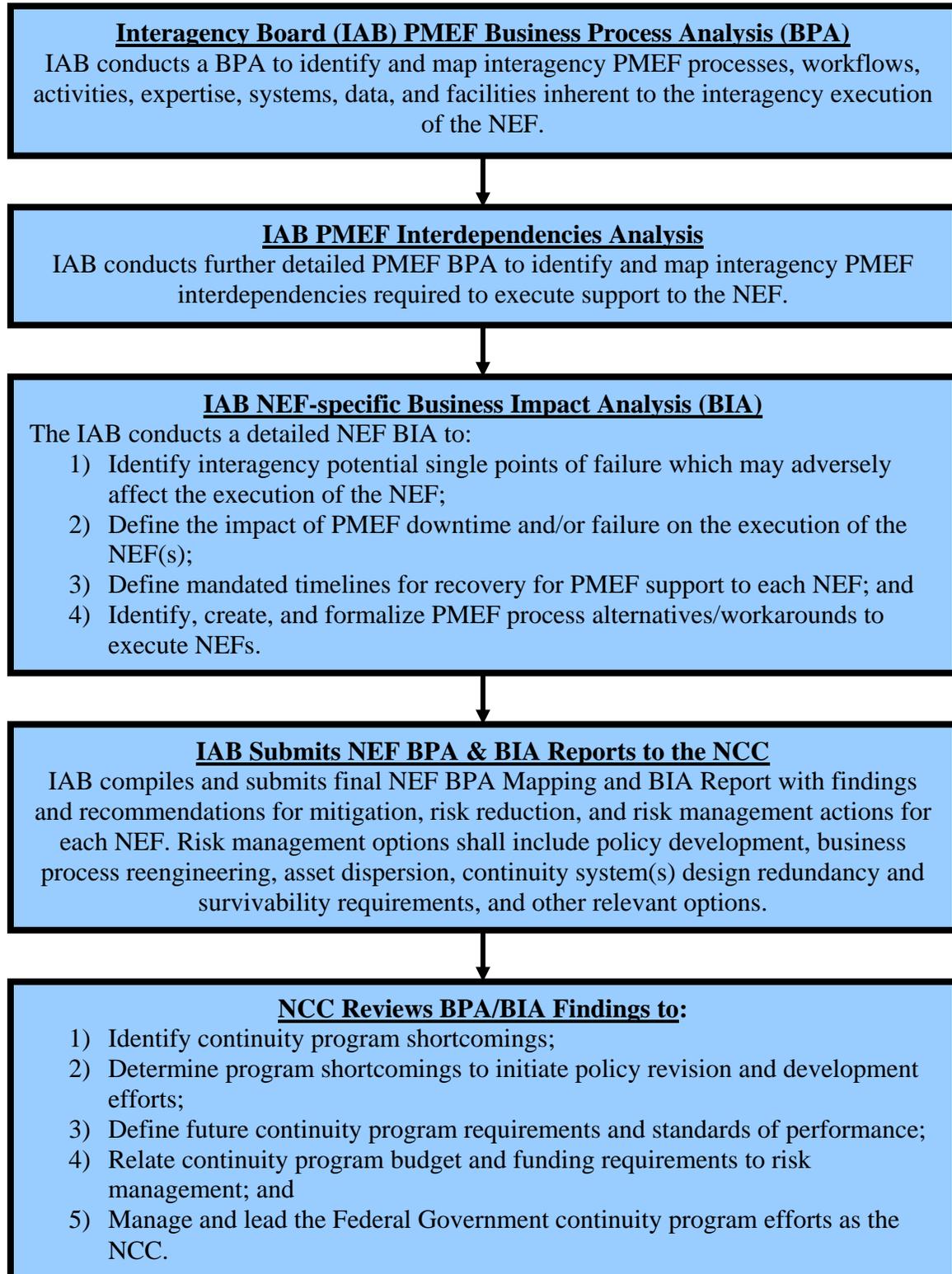


Figure 15

ANNEX E. ORDERS OF SUCCESSION

Agency leadership is responsible for establishing, promulgating, and maintaining orders of succession to key positions. It is critical to have a clear line of succession to office established in the event an agency's leadership becomes debilitated or incapable of performing its legal and authorized duties, roles, and responsibilities. The designation as a successor enables that individual to act on behalf of and exercise the powers of a principal in the event of that principal's death, incapacity, or resignation. Orders of succession enable an orderly and predefined transition of leadership within the organization. Orders of succession are an essential part of an agency's continuity plans and should reach to a sufficient depth and have sufficient breadth—at least three positions deep and geographically dispersed where feasible—to ensure the agency can perform its essential functions while remaining a viable part of the Federal Government during the course of any emergency.

As a minimum, orders of succession must do the following:

1. Establish an order of succession for the position of agency head. There should be a designated official available to serve as acting head of the agency until that official is appointed by the President or other appropriate authority, replaced by the permanently appointed official, or otherwise relieved.
 - a. Geographical dispersion, including of regional, field, or satellite leadership in the standard agency line of succession, is encouraged and ensures roles and responsibilities can transfer in all contingencies.
 - b. Where a suitable field structure exists, appropriate personnel located outside of the subject region should be considered in the order of succession.
2. Establish orders of succession for other key agency leadership positions, including but not limited to administrators, regional or field directors, key managers, other key mission essential personnel or their equivalent positions. Orders of succession should also be established for devolution counterparts in these positions.
3. Describe orders of succession by positions or titles, rather than by the names of the individuals holding those offices. To ensure their legal sufficiency, coordinate the development of orders of succession with the agency's general counsel.
4. Establish the rules and procedures designated officials must follow when facing the issues of succession to office.
5. Include in the succession procedures the conditions under which succession will take place, in accordance with applicable laws and agency or department directives, the method of notification; and any temporal, geographical, or organizational limitations to the authorities granted by the orders of succession.
6. Include orders of succession in the vital records and ensure they are available at all continuity facilities in the event the continuity plan is activated.
7. Revise orders of succession, as necessary, and distribute the revisions promptly as changes occur.

8. Develop and provide a duties and responsibilities briefing to the designated successors to the position of agency head, when named, and other key positions, on their responsibilities as successors and on any provisions for their relocation. Designated successors must receive annual refresher briefings.

ANNEX F. DELEGATIONS OF AUTHORITY

To ensure a rapid response to any emergency and to minimize disruptions that require implementation of continuity plans, agencies should pre-delegate the authority to make policy determinations and decisions, at the headquarters (HQ), regional, field, satellite, and other levels and agency locations, as appropriate. A delegation of authority identifies who is authorized to act on behalf of the agency head or other officials for specified purposes and ensures that designated individuals have the legal authorities to carry out their duties. To the extent possible, these authorities should be identified by title or position, and not by the individual office holder's name. 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 agency's continuity plans and should reach to a sufficient depth and have sufficient breadth—at least three positions deep and geographically dispersed where feasible—to ensure the agency can perform its essential functions while remaining a viable part of the Federal Government during the course of any emergency. To ensure their legal sufficiency and clarity, these delegations of authority must have the following characteristics:

1. A delegation of authority must document in advance (where designated) the legal authority for officials (including those below the level of agency head) to make key policy decisions during a continuity situation.
2. To ensure that an agency's Primary Mission Essential Functions (PMEFs) and Mission Essential Functions (MEFs) are performed, delegations of authority must be planned and documented in advance of an incident and in accordance with applicable laws, including by:
 - a) Delineating the limits of authority and accountability.
 - b) Outlining explicitly in a statement, the authority (including any exceptions to that authority) of an official so designated to exercise agency direction, and the authority of an official to re-delegate functions and activities, as appropriate.
 - c) Defining the circumstances under which delegation of authorities would take effect and would be terminated.
3. Delegations of authority must ensure that those officials who might be expected to assume authorities in a continuity situation are properly informed and trained, as required, to carry out their emergency responsibilities. Training of these officials will be conducted at least annually.
4. Delegations of authority must ensure the orderly (and predefined) transition of leadership, for the position of agency head as well as for key supporting positions, within an agency during an emergency and be closely tied to succession.
5. Include delegations of authority in the vital records and ensure they are available at all continuity facilities in the event the continuity plan is activated.

ANNEX G. CONTINUITY FACILITIES

As part of their continuity plans and procedures, all agencies shall designate: alternate facilities; alternate usages of existing facilities; and as appropriate, virtual office options including telework. In addition, agencies shall prepare their personnel for the possibility of an unannounced relocation to these facilities. Preparations include establishing procedures for the orientation of continuity personnel and for conducting operations and administration at all alternate facilities.

Daily operating facilities must be evaluated for hardness in accordance with Interagency Security Commission Standards or applicable agency standards (i.e., the ability to withstand natural disasters and utility failures and to protect people who need to shelter-in-place). While the hardness of daily operating facilities is a key consideration, alternate facilities must also be identified for the relocation of a limited number of key leaders and staff. Those facilities should replicate essential capabilities by providing systems and configurations that are used in daily activities. Additionally, it is financially prudent to structure and configure alternate facilities such that daily activities can be replaced or augmented with those required during an emergency (often referred to as dual-use facilities).

Planning Requirements

Alternate facilities must provide:

1. Sufficient space, equipment and other resources to sustain the agency's Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs), as appropriate, and Emergency Relocation Group (ERG) and support staff.
2. The capability to perform MEFs and PMEFS as soon as possible after an emergency or other continuity event with minimal disruption of operations and in all cases within 12 hours after an event, the ability to maintain this capability for up to 30 days after an event or until normal business activities can be resumed, and the capability to perform these MEFs under all threat conditions including the possible use of weapons of mass destruction (WMDs). Some essential functions cannot be interrupted and alternate facilities must include support for these continuous operations.
3. Reliable logistical support, services, and infrastructure systems.
4. Consideration for the health, safety, and security of employees who have been relocated to those sites.
5. 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.
6. Computer equipment, software, and other automated data processing equipment necessary to carry out MEFs and PMEFS.
7. Capabilities to access and use vital records necessary to facilitate the performance of essential functions.

Alternate Facility Options

At a minimum, agencies shall identify and maintain an alternate facility. An alternate facility may be classified as one of the following two types:

1. **Hot Site:** An alternate 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.
2. **Warm Site:** An alternate 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.

Alternate facilities may make use of existing agency or other space –

1. **Remote/offsite training facilities.** These facilities may include an agency training facility located near the agency's normal operating facility, but far enough away to afford some geographical dispersion.
2. **Regional or field offices.** Some agencies have a regional office or a field office that could be used as an alternate facility.
3. **Remote headquarters (HQ) operations.** Some agency HQ operations are so extensive that their operations and the facilities required to support them extend beyond the geographic expanse of the agency HQ host city, and necessitate an additional HQ location(s) elsewhere. One of these locations could serve as an alternate facility.
4. **Memorandum of Agreement (MOA)/Memorandum of Understanding (MOU) for co-location with another agency –** One agency may relocate to another agency's facilities. The agency that is relocating could occupy available space in the receiving agency's HQ facility, training facilities, field offices, or other available space.
5. **Space procured and maintained by the General Services Administration (GSA) –** An agency may request the GSA to assign federally owned or leased space to accommodate that agency's need for alternate facilities.
6. **Space procured and maintained by another agency –** Some agencies (other than the GSA) offer space procurement services that could be used by agencies to support the need for alternate facilities.
7. **Participation in a joint-use alternate facility –** With this option, agencies must ensure that shared facilities are not overcommitted during a continuity situation. Several agencies may pool their resources to acquire space they can use jointly as an alternate facility. An agency may co-locate with another agency at an alternate-facility, but each agency should have individually designated space and other resources at that location to meet its own needs (i.e., support its PMEFs and MEFs).
8. **Alternate use of existing facilities –** In certain types of continuity situations (e.g., a pandemic), a combination of facilities may be used to support continuity operations (e.g., social distancing).

In addition to an alternate facility, agencies may consider implementing other or nontraditional continuity facility options including:

1. Virtual offices – To be effective, this option must provide access to vital records and databases to support the agency’s PMEFs and MEFs and the robust communications necessary to sustain an agency’s PMEFs and MEFs.
 - a) Work at home/telework. Many agencies have programs that allow employees to work from home. This capability should be leveraged to allow some continuity personnel to fulfill their MEFs while at home or at another off-site location.
 - b) Telecommuting facilities. These can include federally funded or other telecommuting facilities. These facilities can accommodate, on a prearranged basis, some continuity personnel, to allow them to fulfill their MEFs at those locations.
 - c) Mobile office. This capability includes the use of mobile fly-away kits that can include continuity equipment such as laptop computers, cell phones, and satellite communications equipment, which can be readily transported to a remote location.

Planning Considerations

The following must be considered when identifying and preparing alternate facilities for continuity operations.

1. Location of Facilities. Agencies will conduct an all-hazards risk assessment for all continuity facilities. The assessment will include identification of all hazards that may affect the facility; a vulnerability assessment that determines the effects of all hazards on the facility; a cost-benefit analysis of implementing risk mitigation, prevention, or control measures; and a formal analysis by management of acceptable risk. Alternate facilities must be located in an area where the potential disruption of the agency’s ability to initiate and sustain operations is minimized. When identifying and preparing alternate facilities, maximum use should be made of existing local or field infrastructures, including consideration for other supporting options such as telecommuting locations, work-at-home/telework agreements, virtual offices, and joint or shared facilities. Additionally, alternate facilities:
 - a. Must be operational as soon as possible upon continuity activation with minimal disruption of operations, but in all cases within 12 hours after activation of a continuity plan, and be capable of sustaining operations for up to 30 days after an incident or until normal business operations can be resumed. Agencies will identify essential functions that cannot be disrupted for any period of time and must be continued under all conditions in their continuity plans, and must provide support for their performance from alternate facilities.
 - b. Must have sufficient distance between the facility location or threatened area and other facilities (hazardous materials sites, nuclear power plants) or locations (areas subject to natural disasters such as hurricanes and earthquakes) that are potential sources of disruptions or threats.
 - c. Must have access to essential support resources such as food, water, fuel, medical facilities, and municipal services (e.g., fire, police).

-
- d. Accessibility will include a defined transportation support plan that describes procedures for events with both warning and no warning.
 - e. Should be selected in locations that provide the alternate sites with power, telecommunication services, and Internet access, separate from those grids that provide their services to the primary facility, whenever possible.
2. Construction. Facilities should be selected and constructed so that they are not uniquely susceptible to risks associated with such natural disasters as earthquakes, tornadoes, hurricanes, or floods. Alternate facilities must have emergency/back-up power capability, so that essential functions and operations can continue in the event the primary source of power is disrupted.
 3. MOA/MOU. If the alternate facility is neither owned nor leased by the agency, a signed MOA/MOU must be prepared with the owner or occupant of the facility. This MOA/MOU must be reviewed annually. It is recommended that agencies coordinate with GSA for assistance in identifying relocation sites. MOAs/MOUs should specify:
 - a. The required activation time between notifying the owner/occupant of the requirement to use the facility and the facility being available for occupancy by the agency as an alternate.
 - b. Space and services to be provided at the facility.
 - c. Sole use of allocated space by the agency during the period of occupancy.
 4. Space. An agency's alternate facility space requirements must be sufficient to support all of the agency's continuity staffing requirements. Contiguous space is desirable; however, noncontiguous space may be acceptable if there is adequate communications between ERG members.
 5. Preparation. After selecting appropriate sites for continuity operations, pre-positioning of critical resources, coordination with the site facility managers, and agreements between the agency and property owners are necessary to ensure the continued availability of facility space and services. Agencies must have all necessary supplies and equipment pre-positioned or have detailed site preparation and activation plans in order to achieve full operational capability within 12 hours of notification.
 6. Billeting. All continuity plans will address housing to support continuity personnel at or near the alternate facility site (e.g., billeting within facility; other locations, including motels; or at ERG members' homes if within commuting distance to the alternate facility).
 7. Site Transportation. Transportation resource requirements, including transportation to/from the site, and on the site should be included, as applicable.
 8. Communications. The communications resources at the alternate facility must be sufficient to enable performance of all essential functions. This includes providing sufficient quantity and mode/media to allow for effective interaction with other agency elements (e.g., regional offices), other agencies, stakeholders and other recipients of the agency's essential functions or services, and other government and private sector organizations (including key operations centers) critical to the performance of that
-

agency's essential functions. Secure and non-secure communications requirements should be incorporated, as applicable.

9. **Security.** Procedures for the safety and security of relocated personnel, information, data, and equipment must be included in all continuity plans. Alternate facilities must afford sufficient levels of physical and information security to protect against all threats as identified in the facility's risk assessment and physical security surveys by the agency's security office, the Federal Protective Service, or a qualified security contractor. This includes sufficient personnel to provide perimeter, access, and internal security, as required by agency policy. Technologies that control site access, conduct site surveillance, and provide early warning of unauthorized intrusion, should also be considered as part of the alternate facility's physical security program.
10. **Life Support.** Life support items (e.g., food, water, medical services, sanitation, hygiene, power) should be readily available and in sufficient quantities to sustain, at a minimum, 30 days of operations, with the capability to sustain operations beyond that period for extended-duration events such as a pandemic. In addition, personnel and support items such as medical supplies, medical records, and housekeeping supplies should be maintained at the facility or brought to the facility during relocation.

The Acquisition Process

The process of acquiring an alternate facility includes: (1) identifying alternate facility requirements, (2) selecting and acquiring the alternate facilities, and (3) reevaluating alternate facilities. These steps should be performed in consultation with the GSA whenever possible.

Once selected, alternate facilities must be periodically reevaluated for their suitability and functionality. This should be done at least annually and whenever the agency's continuity plans are reviewed and updated, to ensure that the facilities meet the agency's continuity requirements.

The Reporting Process

GSA will create and maintain a central database of all alternate facilities. All agencies are required to identify their alternate facilities and provide the necessary data on those facilities to GSA. To support this requirement, all agencies will report the locations of their alternate facility(ies) to GSA's Emergency Management Office or their Regional GSA Office, as appropriate, on GSA Alternate Facility Reporting Form, SF-336.

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 agency's ability to execute its essential functions at its headquarters (HQ) and at its alternate or other continuity facilities, as well as the ability of the agency'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 must support full connectivity, under all conditions, among key government leadership, internal elements, other agencies, critical customers, and the public.

In accordance with the National Communications System's (NCS) Directive 3-10, NCS Manual 3-10-1, and other established communications requirements, an agency must:

1. Implement minimum communications requirements for its HQs and its alternate and other continuity facilities, as appropriate, which support the continuation of that agency's Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs);
2. Possess interoperable and available communications capabilities in sufficient quantity and mode/media, and that are commensurate with that agency's responsibilities during conditions of an emergency;
3. Possess communications capabilities that can support the agency's senior leadership while they are in transit to alternate facilities;
4. Ensure that the communications capabilities required by this Directive are maintained and readily available for a period of sustained usage of no less than 30 days or until normal operations can be reestablished, and that all continuity staff are properly trained, as appropriate, in the use of these communications capabilities;
5. Satisfy the requirement to provide assured and priority access to communications resources; and
6. Have sufficient communications capabilities to accomplish the agency's essential functions from an alternate facility. If the agency's alternate facility is shared with another agency, also have a signed agreement with that agency which ensures that each has adequate access to communications resources.

All agencies that support National Essential Functions (NEFs) shall possess, operate, and maintain, or have dedicated access to, communications capabilities at both their HQ and alternate facility locations, as well as mobile communications capabilities, to ensure the continuation of those agencies' essential functions across the full spectrum of hazards, threats, and emergencies, including catastrophic attacks or disasters.

Those agencies that do not support NEFs shall possess, operate, and maintain, or have dedicated access to, communications capabilities at both their HQ and alternate facility locations, as well as mobile communications capabilities as required, to ensure the continuation of those agencies' essential functions.

All agencies will review their continuity communications programs to ensure they are fully capable of supporting pandemic and other related emergencies and give full consideration to supporting social distancing operations including telework and other virtual offices.

Agencies may expand or migrate, as appropriate, their communications capabilities to make use of emerging technologies, but agencies should ensure that any additional communications capabilities they may obtain are compatible with existing equipment and complement the established requirements.

The NCS, a component of the Department of Homeland Security's National Protection and Programs Directorate, is responsible for:

1. Within 30 days after receipt of technical requirements from the Office of Science and Technology Policy (OSTP), as Executive Agent of the National Communications System (NCS), providing the Director of OSTP and Department of Defense (DOD) with an implementation plan for a comprehensive Continuity Communications Architecture (CCA), which shall include the minimum requirements necessary to finalize selection of a secure communications system by DOD.
2. Within 90 days after receipt of technical requirements from OSTP, through the NCS, developing, implementing, and beginning maintenance of a comprehensive CCA.

Agencies may request an exemption from one or more of these minimum communications requirements by submitting a request by letter through the Office of Manager of the NCS to the National Continuity Coordinator (NCC). 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. VITAL RECORDS MANAGEMENT

The identification, protection, and ready availability of vital records, databases, and hardcopy documents needed to support Primary Mission Essential Functions (PMEFs) and Mission Essential Functions (MEFs) under the full spectrum of all-hazards emergencies are critical elements of a successful continuity plan and program.

In this document, “vital records” refers to information systems and applications, electronic and hardcopy documents, references, and records needed to support PMEFs and MEFs during a continuity event.

Categories of vital records include the following:

Emergency Operating Records. These include records and databases essential to the continued functioning or the reconstitution of an agency during and after a continuity event. 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 agency’s continuity personnel with the guidance they need to conduct operations during a continuity situation and to resume normal operations at the conclusion of that situation. Agencies must identify and preposition Emergency Operating Records needed to continue essential functions.

Rights and Interests Records. These include records critical to carrying out an agency’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 agency’s activities. These records include those with such value that their loss would significantly impair the execution of essential agency functions, to the detriment of the legal or financial rights and entitlements of the agency 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 alternate continuity facility.

Other vital records required to support PMEFs and MEFs will also be included in an agency’s continuity planning and preparedness.

Each agency has different functional responsibilities and business needs. An agency must decide which records are vital to its operations, and then must assign responsibility for those records to the appropriate personnel, who may be a combination of continuity personnel, personnel in the chief information officer’s department, and records management personnel. An effective vital records program should have the following characteristics:

1. An official vital records program:
 - a. Identifies and protects those records that specify how an agency will operate in an emergency or disaster.
 - b. Identifies those records necessary to the agency’s continuing operations.

- c. Identifies those records needed to protect the legal and financial rights of the Government and citizens.
 2. A vital records program must be incorporated into the overall continuity plans, and it needs a clear authority to include:
 - a. Policies.
 - b. Authorities.
 - c. Procedures.
 - d. The written designation of a vital records manager.
 3. As soon as possible after activation of continuity plans, but in all cases within 12 hours of such activation, continuity personnel at the alternate facility must have access to the appropriate media for accessing vital records, such as:
 - a. A local area network.
 - b. Electronic versions of vital records.
 - c. Supporting information systems and data.
 - d. Internal and external e-mail and e-mail archives.
 - e. Hard copies of vital records.
 4. Agencies should strongly consider multiple redundant media for storing their vital records.
 5. Agencies must maintain a complete inventory of records (such as those identified in the previous paragraphs on Emergency Operating Records and Rights and Interests Records), along with the locations of and instructions on accessing those records. This inventory will be maintained at a back-up/offsite location to ensure continuity if the primary site is damaged, destroyed, or unavailable. Agencies should consider maintaining these inventories at a number of different sites to support continuity operations.
 6. Agencies must conduct a vital records and database risk assessment to:
 - a. Identify the risks involved if vital records are retained in their current locations and media, and the difficulty of reconstituting those records if they are destroyed.
 - b. Identify offsite storage locations and requirements.
 - c. Determine if alternative storage media is available.
 - d. Determine requirements to duplicate records and provide alternate storage locations to provide readily available vital records under all conditions.
 7. Appropriate protections for vital records will include dispersing those records to other agency 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. Microforms, paper photographs, and computer disks, tapes, and drives, all require different methods of protection. Some of these media may also require equipment to facilitate access.
-

8. At a minimum, vital records must be annually reviewed, rotated, or cycled so that the latest versions will be available.
9. A vital records plan packet must be developed and maintained. The packet will include:
 - a. A hard copy or electronic list of key agency personnel and continuity personnel with up-to-date telephone numbers.
 - b. A vital records inventory with the precise locations of vital records.
 - c. Updates to the vital records.
 - d. Necessary keys or access codes.
 - e. Alternate facility locations.
 - f. 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).
 - g. Lists of records recovery experts and vendors.
 - h. A copy of the agency’s continuity plans.

This packet will be annually reviewed with the date and names of the personnel conducting the review documented in writing to ensure that the information is current. A copy will be securely maintained at the agency’s alternate facilities and other locations where it is easily accessible to appropriate personnel when needed.

10. A vital records program must include a training program for all staff to include periodic briefings to managers about the vital records program and its relationship to their vital records and business needs. Staff training should focus on identifying, inventorying, protecting, storing, accessing, and updating the vital records.
11. A vital records program must include an annual review of the program to address new security issues, identify problem areas, update information, and incorporate any additional vital records generated by new agency programs or functions or by organizational changes to existing programs or functions. The review will provide an opportunity to familiarize staff with all aspects of the vital records program. It is appropriate to conduct a review of the vital records program in conjunction with continuity exercises.
12. There must be annual testing of the capabilities for protecting classified and unclassified vital records and for providing access to them from the alternate facility.

Table 2 may be useful in assisting agencies in identifying and managing their vital records.

Vital Records	Form of Record (e.g., hardcopy, electronic)	Pre-Positioned at Alternate Facility	Hand Carried to Alternate Facility	Storage Location(s)	Maintenance Frequency
		<input type="checkbox"/>	<input type="checkbox"/>		
		<input type="checkbox"/>	<input type="checkbox"/>		
		<input type="checkbox"/>	<input type="checkbox"/>		

Table 2: Identification of Vital Records

ANNEX J. HUMAN CAPITAL

In a continuity event, continuity personnel and other special categories of employees will be activated by an agency to perform their assigned response duties. Continuity personnel will also be referred to as members of the emergency relocation group (ERG). In addition to supporting the human capital needs of the agency's continuity personnel, agencies are responsible for managing their other human capital resources—those employees who have not been designated as continuity or ERG personnel, but who will nevertheless be potentially affected by a continuity event. Agency plans and procedures for these employees should be addressed in the continuity plans as well as in other types of emergency response planning documents, such as the agency's Occupant Emergency Plan (OEP) or shelter-in-place plans.

Because of the need for agencies to be prepared for all-hazards emergencies and disasters, an agency must ensure that its human capital strategies for its continuity staff are adaptable to changing circumstances and a variety of emergencies, and that these strategies and procedures are regularly reviewed and updated as appropriate, as part of the agency's Corrective Action Program (CAP).

This annex is divided into three sections: Continuity Leadership and Staff; All Staff; and Human Capital Considerations.

Continuity Personnel

This section addresses those employees (i.e., Continuity or ERG personnel) who perform the agency's essential functions during a continuity event. The following activities are associated with planning and preparedness for continuity personnel:

1. **Agencies must develop and implement a process to identify, document, communicate with and train continuity personnel.** The identification of an agency's continuity personnel is a critical part of ensuring that an agency can successfully respond to a continuity event. Specific factors an agency should consider in developing and implementing this process include identifying:
 - a. Personnel who perform essential functions as determined through the business process analysis (BPA) (discussed in Annex D).
 - b. Personnel who perform the supporting tasks that enable the performance of essential functions.
 - c. Skill sets necessary to perform specific essential functions or to support tasks that enable the performance of those essential functions.

Each agency head has the authority to identify and designate those personnel that the agency head judges to be critical to agency operations in any given emergency situation such as a continuity event. There are no standard definitions or categories in this regard, and agency heads (or their designees, as applicable) are free to make such determinations based on the agency's unique mission requirements and circumstances; such designations may even vary according to the particular nature of an emergency.

By identifying not only the personnel who currently perform essential functions or supporting tasks but also those who possess the skill sets necessary to perform these functions and tasks, an agency can reach beyond that set of individuals who traditionally perform these roles to respond during a continuity event that may require augmentation of the standing cadre of continuity personnel.

Agencies must ensure that continuity personnel are officially informed of their roles or designations by providing documentation to ensure that continuity personnel know and accept their roles and responsibilities. This process and its supporting documentation will help ensure that all continuity personnel receive the necessary guidance and support and know prior to, during, and after a continuity event what the agency expects of them. Agencies may customize this process to best suit their specific needs and requirements.

In addition to their continuity planning requirements, continuity personnel must understand their roles and responsibilities and participate in their agency's continuity tests, training, and exercise (TT&E) program.

- 2. Agencies must provide guidance to continuity personnel on individual preparedness measures they should take to ensure response to a continuity event.** Continuity personnel have individual and specific responsibilities outside of their professional obligations. By taking personal preparedness measures, such as a personal readiness kit or family preparedness planning, continuity personnel will be able to respond to a continuity event with a greater level of confidence that they can meet their individual responsibilities and obligations. Continuity personnel must implement personal preparedness measures to ensure their ability to respond to a continuity event.

All Staff

This section addresses the continuity planning and programming concerns that are applicable to all agency employees regardless of their connection to the ERG. The following activities are associated with continuity planning and preparedness for all agency staff regardless of their status with the ERG:

- 3. Agencies must implement a process to communicate the agency's operating status to all staff.** Agencies should follow the dismissal or closure procedures established for the facility or geographic region affected by an emergency situation that prevents significant numbers of employees from reporting for work on time or that requires agencies to close all or part of their activities. Agencies in the Washington, DC, area should follow the "Washington, DC, Area Dismissal or Closure Procedures" which are available through the U.S. Office of Personnel Management Operating Status for the Washington, DC, area on the OPM website: <http://www.opm.gov/emergency>. Federal Executive Boards (FEBs) and Federal Executive Associations (FEAs) should coordinate similar dismissal or closure procedures in other major metropolitan areas. In addition, agencies must communicate how, and the extent to which, employees are expected to remain in contact with their agencies during any closure situation.

4. **Agencies must implement a process to contact and account for all staff in the event of an emergency.** Agencies should have procedures in place to contact employees in the event of an emergency. Agencies should establish alternative means for employees to contact the agency in the event an emergency causes a disruption to the regular means of communication with the agency. These communications could be conducted by either establishing a toll free telephone number or a website that would allow employees to notify the agency of their status.

Human Capital Considerations

This section addresses the unique human capital related requirements and other issues that are required to support an effective continuity plan and program. An agency's Continuity Coordinator (or continuity manager) should work closely with the agency's Chief Human Capital Officer or Director of Human Resources to resolve human capital issues related to a continuity event. Human capital issues can be solved typically at the agency level through the agency's Chief Human Capital Officer or Director of Human Resources, or their designees, using available laws, U.S. Office of Personnel Management regulations and guidance, as well as agency implementing instructions. The planning and preparedness related to human capital for a continuity event includes the following activities:

5. **Agencies must identify a human capital liaison from the agency's human resources staff to work with the Continuity Coordinator or continuity manager when developing the agency's emergency plans.** An agency's Continuity Coordinator should work closely with the agency's Chief Human Capital Officer or Director of Human Resources to resolve human capital issues related to a continuity event. The Chief Human Capital Officer or Director of Human Resources will ensure that the agency's policies remain current and relevant to changing environments or evolving threats. An agency's continuity programs, plans, or procedures should include agency-specific guidance and direction for continuity personnel on a wide range of human capital areas. Additional guidance is available at the U.S. Office of Personnel Management website at <http://www.opm.gov>.
6. **Agencies must implement a process to communicate their human capital guidance for emergencies (pay, leave, staffing and other human resources flexibilities) to managers and make staff aware of that guidance in an effort to help agencies continue essential functions during an emergency.** Working with the Chief Human Capital Officer or Director of Human Resources, agencies must institute a process to communicate their human capital guidance for emergencies to managers, such as guidance on pay, leave, work scheduling, benefits, telework, hiring, etc., authorities and flexibilities. Pay, leave, staffing, and other human resources flexibilities available to agencies during an emergency are available through the agencies' human capital or human resources offices and on the U.S. Office of Personnel Management website at <http://www.opm.gov/emergency>. In addition to communicating their human capital guidance to managers, agencies must institute methods for staff to become aware of and

familiar with the human capital guidance during emergencies such as utilizing an intranet website or employee orientation briefing.

Agency Continuity Coordinators should consult with their Chief Human Capital Officer or Director of Human Resources on ways to meet the six requirements of human capital planning for continuity identified above. The U.S. Office of Personnel Management will work with the Chief Human Capital Officers Council and Directors of Human Resources to provide additional guidance as necessary.

ANNEX K. TEST, TRAINING, AND EXERCISE (TT&E) PROGRAM

An effective TT&E program is necessary to assist agencies to prepare and validate their organization's capabilities and program, and to the Federal executive branch's ability to perform Primary Mission Essential Functions (PMEFs) and Mission Essential Functions (MEFs) during any emergency. This requires the identification, training, and preparedness of personnel capable of performing their continuity responsibilities and implementing procedures to support the continuation of agency essential functions.

The testing, training, and exercising of continuity capabilities is essential to demonstrating, assessing, and improving an agency's ability to execute its continuity program, plans, and procedures. Training familiarizes continuity personnel with their roles and responsibilities in support of the performance of an agency's essential functions during a continuity event. Tests and exercises serve to assess, validate, or identify for subsequent correction, all components of continuity plans, policies, procedures, systems, and facilities used in response to a continuity event. Periodic testing also ensures that equipment and procedures are kept in a constant state of readiness. An agency's TT&E program should be part of a multiyear TT&E plan that addresses continuity TT&E requirements, resources to support TT&E activities, and a TT&E planning calendar. The following details the specific requirements for each component:

Testing

An agency's test program must include:

1. Annual testing of alert, notification, and activation procedures for continuity personnel, and quarterly testing of such procedures for continuity personnel at agency headquarters.
2. Annual testing of plans for recovering vital records (both classified and unclassified), critical information systems, services, and data.
3. Annual testing of primary and backup infrastructure systems and services (e.g., power, water, fuel) at alternate facilities.
4. Annual testing and exercising of required physical security capabilities at alternate facilities.
5. Testing and validating equipment to ensure the internal and external interoperability and viability of communications systems, through monthly testing of the continuity communications capabilities outlined in Annex H (e.g., secure and nonsecure voice and data communications).
6. Annual testing of the capabilities required to perform an agency's MEFs, as identified in the business process analysis (BPA).
7. Conducting annual testing of internal and external interdependencies identified in the agency's continuity plan, with respect to performance of an agency's and other agencies' MEFs.
8. A process for formally documenting and reporting tests and their results.
9. Reporting the test results as directed by Department of Homeland Security (DHS) /Federal Emergency Management Agency (FEMA).

Training

An agency's training program must include:

1. Annual continuity awareness briefings (or other means of orientation) for the entire workforce.
2. Annual training for personnel (including host or contractor personnel) who are assigned to activate, support, and sustain continuity operations.
3. Annual training for the agency's leadership on that agency's PMEFs and MEFs, including training on their continuity responsibilities.
4. Annual training for all agency personnel who assume the authority and responsibility of the agency's leadership if that leadership is incapacitated or becomes otherwise unavailable during a continuity situation.
5. Annual training for all predelegated authorities for making policy determinations and other decisions, at the headquarters, field, satellite, and other organizational levels, as appropriate.
6. Personnel briefings on agency continuity plans that involve using, or relocating to, alternate facilities, existing facilities, or virtual offices.
7. Annual training on the capabilities of communications and information technology (IT) systems to be used during a continuity event.
8. Annual training 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 situation.
9. Annual training on an agency's devolution option for continuity, to address how each agency will identify and conduct its essential functions during an increased threat situation or in the aftermath of a catastrophic emergency.
10. Annual training for all reconstitution plans and procedures to resume normal agency operations from the original or replacement primary operating facility.

Training must prepare continuity personnel to respond to all emergencies and disasters and ensure performance of the agency's essential functions. These include interdependencies both within and external to the agency. As part of its training program, the agency must document the training conducted, the date of training, those completing the training, and the training facilitator/instructor. Agencies must also submit an annual report on their training program to FEMA. Specific reporting requirements and guidance shall be updated annually by FEMA.

Exercises

An agency'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. Agency's should refer to HSEEP for additional exercise and evaluation guidance.

An agency's exercise program must include:

1. Compliance with the DHS-mandated National Exercise Program (NEP), as appropriate.
2. An annual opportunity for continuity personnel to demonstrate their familiarity with continuity plans and procedures and to demonstrate the agency's capability to continue its essential functions.

3. An annual exercise that incorporates the deliberate and preplanned movement of continuity personnel to an alternate facility or location.
4. An opportunity to demonstrate intra- and interagency communications capabilities.
5. An opportunity to demonstrate that backup data and records required to support essential functions at alternate facilities or locations are sufficient, complete, and current.
6. An opportunity for continuity personnel to demonstrate their familiarity with the reconstitution procedures to transition from a continuity environment to normal activities when appropriate.
7. An opportunity for continuity personnel to demonstrate their familiarity with devolution procedures.
8. 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 agency's continuity plan.
9. A cycle of events that incorporates evaluations, after-action reports, and lessons learned into the development and implementation of a corrective action program (CAP).
10. Organizational participation: conducting and documenting annual assessments of their continuity TT&E programs and continuity plans and programs, and then reporting these findings as directed to FEMA.
11. Organizational assistance to FEMA in conducting annual full-scale continuity exercises and biennial assessments of the agency's continuity program with reports submitted to the National Continuity Coordinator (NCC) and the President.
12. Each department and agency shall develop a CAP to assist in documenting, prioritizing, and resourcing continuity issues identified during TT&E, assessments, and emergency operations. The purpose of a CAP is to accomplish the following:
 - a. Identify continuity deficiencies and other areas requiring improvement and provide responsibilities and a timeline for corrective action.
 - b. Identify program and other continuity funding requirements for submission to department and agency leadership and Office of Management and Budget (OMB).
 - c. Identify and incorporate efficient acquisition processes, and where appropriate, collect all interagency requirements into one action.
 - d. Identify continuity personnel requirements for department and agency leadership and their supporting Human Resource Offices and the U.S. Office of Personnel Management (OPM).

The NEP, under the leadership of the Secretary of Homeland Security, is a mechanism for examining the preparation of the United States Government and its officers and other officials, and for adopting policy changes that might improve such preparations. The principal focus of the NEP is a series of exercises designed for heads of agencies and other key officials, which examines and evaluates emerging national-level policy issues. The NEP also addresses the coordination of exercise efforts.

The NEP does not preclude or replace exercise programs conducted by individual agencies, but it allows and encourages agencies to align their exercise programs to United States government-wide priorities. This may result in internal exercises that serve as building blocks *toward* an agency's participation in NEP events, or it may result in proposals for incorporating an individual agency's continuity exercises *within* a NEP event. The 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 NEP framework.

Separate from their participation in NEP events, agencies must develop and maintain a continuity TT&E program for conducting and documenting TT&E activities.

ANNEX L. DEVOLUTION OF CONTROL AND DIRECTION

Devolution planning supports overall continuity planning and addresses catastrophes and other all-hazards emergencies that render an agency's leadership and key staff unavailable to or incapable of performing its essential functions from either the agency's primary or alternate facilities. Devolution planning also addresses notice and no notice events. A continuity plan's devolution option should be developed so that it addresses how an agency will identify and transfer its essential functions and/or leadership authorities away from the primary facility or facilities, and to a location that offers a safe and secure environment in which essential functions can continue to be performed. The devolution option may be used when the agency's alternate facility is not available, or the option can be activated as a continuity measure.

At a minimum a devolution plan will:

1. Include the following elements of a viable continuity capability: program plans and procedures, budgeting and acquisitions, essential functions, orders of succession and delegations of authority specific to the devolution site, interoperable communications, vital records management, staff, test, training, and exercise (TT&E), and reconstitution.
2. Identify essential functions, define tasks that support those essential functions, and determine the necessary resources to facilitate those functions' immediate and seamless transfer to the devolution site.
3. Include a roster that identifies fully equipped and trained personnel who will be stationed at the designated devolution site and who will have the authority to perform essential functions and activities when the devolution option of the continuity plan is activated.
4. Identify what would likely activate or "trigger" the devolution option.
5. Specify how and when direction and control of agency operations will be transferred to and from the devolution site.
6. List the necessary resources (i.e., equipment and materials) to facilitate the performance of essential functions at the devolution site.
7. Establish and maintain reliable processes and procedures for acquiring the resources necessary to continue essential functions and to sustain those operations for extended periods.
8. Establish and maintain a capability to restore or reconstitute agency authorities to their pre-event status upon termination of devolution.

Devolution plans, responsibilities, and capabilities will include all elements of continuity planning including tests, annual training of devolution staff, and at a minimum, biennial exercises to ensure devolution capabilities are prepared and capable of performing an agency's essential functions.

All devolution preparedness activities will be documented in writing with dates of TT&E and names of staff participating in the TT&E.

A corrective action program (CAP) will be established and documented to support an agency's devolution program.

ANNEX M. RECONSTITUTION OPERATIONS

Agencies must identify and outline a plan to return to normal operations once agency heads or their successors determine that reconstitution operations for resuming normal business operations can be initiated. Agencies must:

1. Provide an executable plan for transitioning back to efficient normal operational status from continuity operations status, once a threat or disruption has passed.
2. Coordinate and pre-plan options for agency reconstitution regardless of the level of disruption that originally prompted the agency to implement its continuity plans. These options must include moving operations from the continuity or devolution location to either the original operating facility or, if necessary, to a new operating facility.
3. Outline the necessary procedures, whether under a standard continuity operations scenario or under a devolution scenario, for conducting a smooth transition from the relocation site to a new facility.

Implementation actions associated with reconstitution include:

1. Informing all personnel that the actual emergency, or the threat of an emergency, no longer exists, and instructing personnel on how to resume normal operations.
2. Supervising either an orderly return to the normal operating facility or a move to another temporary facility or to a new permanent operating facility.
3. Verifying that all systems, communications, and other required capabilities are available and operational and that the agency is fully capable of accomplishing all essential functions and operations at the new or restored facility.
4. Organizations are required to notify their agency HQ upon continuity reconstitution. Agency HQ Points of Contact (POCs) must notify the FOC at 540.665.6100 or at 800.634.7084. Agency HQ POCs shall submit a Continuity Status Reporting Form only if it contains more information beyond what has been reported to the FOC, to fema-ncp-coop@dhs.gov or Fax to 940.323.2822, using the form and procedures provided by FEMA's National Continuity Programs Directorate.
5. Conducting an after-action review of the effectiveness of the continuity plans and procedures, identifying areas for improvement, documenting these in the agency's corrective action program (CAP), and then developing a remedial action plan as soon as possible after the reconstitution.
6. Identifying which (if any) records were affected by the incident, and working with the records office (or similar function in the agency) to ensure an effective transition or recovery of vital records and databases and other records that had not been designated as vital records.

ANNEX N. CONTINUITY PLAN OPERATIONAL PHASES AND IMPLEMENTATION

An agency must be prepared to implement executive decisions that are based upon a review of the emergency, and that then determine the best course of action based on the agency's readiness posture. The agency should integrate implementation procedures and criteria into their continuity plans. The agency's continuity plan must address four phases of: (1) readiness and preparedness, (2) activation and relocation, (3) continuity operations, and (4) reconstitution.

Readiness and Preparedness

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

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

1. An agency receives, or the region the agency is located in receives, notification of a credible threat, which leads the agency to enhance its readiness posture and prepare to take actions as necessary.
2. An agency experiences an emergency or a disruption that does not require movement of all continuity personnel to an alternate site. Some disruptions may require that key personnel remain onsite to conduct essential functions; other disruptions may prevent some or all personnel from getting to the agency's primary location; and yet others may require implementing a social distancing strategy which would require the use of primary, alternate and other relocations, such as telework.
3. An agency headquarters (HQ) continuity staff or facilities are unavailable, necessitating a shift of operations to a regional, field or other location (devolution).
4. A single agency facility is temporarily unavailable, and the agency either accommodates that facility's operations and personnel at another of its own facilities, or transfers those operations and personnel to a facility of another agency.
5. Many, if not all, agencies must evacuate the immediate or larger geographically affected area.

Organizations outside the National Capital Region (NCR) may consider creating a "continuity readiness posture" similar to the executive branch's Continuity of

Government Readiness Conditions (COGCON) system for the NCR, which is presented in Table 3.

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)

Table 3: COGCON Matrix

Activation and Relocation (0-12 Hours)

The agency will provide a process or methodology for attaining operational capability at all continuity sites as soon as possible and with minimal disruption to operations, but in all cases within 12 hours of activation. Agencies will also identify those essential functions that must be continued without disruption and will ensure these can be conducted, under all conditions. The process should include the activation of plans, procedures, and schedules for the continuation of essential functions, as well as for the personnel, vital records and databases, and equipment involved with these functions, with minimal disruption. The activation and relocation phase includes the following activities:

1. The occurrence of an event or the threat of an event.
2. Review, analysis, and decision to activate continuity plans.
3. Alert and notification of continuity personnel.
4. Relocation, if necessary, to alternate or other continuity facilities.
5. An accountability analysis of continuity personnel.
6. Identification of available leadership.
7. Determination and reporting of operational capabilities to the FEMA Operations Center (FOC).

Organizations are required to notify their agency HQ upon activation of continuity plans. Agency HQ Points of Contact (POCs) must notify the FOC at 540.665.6100 or at 800.634.7084, and submit a Continuity Status Reporting Form to fema-ncp-coop@dhs.gov or Fax to 940.323.2822, using the form and procedures provided by FEMA's National Continuity Programs Directorate, of any activation of continuity plans (regardless of the agency's location) and of the time of execution or activation of call-down procedures. The POCs should also courtesy copy the National Operations Center (NOC).

Activation and relocation plans or procedures should include the following:

1. A decision matrix for continuity plan activation:
 - a. With warning during duty hours and non-duty hours.
 - b. Without warning during duty hours and non-duty hours.
 2. Notification of:
 - a. Alternate facilities and on site support teams.
 - b. The FOC (by the agency's HQ) of continuity plan activation and relocation (Subordinate agency organizations will notify their respective agency HQ of continuity plan activation and relocation, and HQ will in turn notify the FOC).
 - c. Other POCs, as appropriate.
 - d. Employees (continuity personnel and non-deployed personnel).
 3. Instructions on moving to an alternate facility, including directions to the site(s) and maps of routes from the primary location to the alternate or other continuity facility or location.
 4. Identification of what drive-away kits should contain and how those kits will be maintained.
 5. Instructions on moving vital records (those that have not been prepositioned) from the primary to the alternate facility.
-

6. Instructions on procuring necessary equipment/supplies that are not already in place.

Continuity Operations

This phase includes the following activities to continue essential functions:

1. Accounting for all agency personnel.
2. Performing essential functions (which depend on the situation).
3. Establishing communications with supporting and supported agencies, customers, and stakeholders.
4. Preparing for the reconstitution of the Agency.

Plans or procedures will include:

1. Reception in-processing and accounting for continuity personnel.
2. Transition of responsibilities to the deployed continuity personnel.
3. Guidance for nondeployed personnel.
4. Identification of replacement personnel and augmentees, as necessary.
5. Execution of all essential functions at the alternate facility.
6. Activation of processes and procedures to acquire the resources necessary to continue essential functions and to sustain operations.
7. Notification of agencies that the affected agency interacts with, customers, and stakeholders of activation of continuity plans and status (agency headquarters will notify the FOC and all other appropriate POCs of the agency's alternate location, operational and communications status, and anticipated duration of relocation, if known. The FOC will notify agencies of any additional continuity reporting requirements).
8. Redeployment plans for phasing down alternate facility operations and returning operations, personnel, records, and equipment to the primary or other operating facility, when appropriate.

Reconstitution

Reconstitution is normally conducted using a priority-based phased approach, in which most critical functions are transferred last. Those functions that were discontinued because of the emergency should be reconstituted first. All personnel should be informed that the necessity for continuity operations no longer exists. Instructions for resumption of normal operations are provided, including supervising an orderly return to the normal operating facility, moving to another temporary facility, or to a new permanent facility. All organizations will report their location status to higher HQ. HQ elements will report movement status to the FOC. The FOC will relay this information to the NOC and the FEMA National Continuity Programs Directorate. The process of reconstitution will generally start immediately after an event concludes, and can run concurrently with the recovery process. 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.
5. Implementing a priority-based phased approach to reconstitution.

There should be an after-action review of the effectiveness of continuity plans and procedures as soon as possible, including an identification of aspects of the plans and procedures that need to be corrected, followed by development of a corrective action program (CAP).

ANNEX O. LIST OF ACRONYMS

APHS/CT	Assistant to the President for Homeland Security and Counterterrorism
APNSA	Assistant to the President for National Security Affairs
BIA	Business Impact Analysis
BPA	Business Process Analysis
CAG	Continuity Advisory Group
CAP	Corrective Action Program
CCA	Continuity Communications Architecture
CCAB	Continuity Communications Architecture Board
CI/KR	Critical Infrastructure and Key Resources
COG	Continuity of Government
COGCON	Continuity of Government Readiness Conditions
COOP	Continuity of Operations
CPCC	Continuity Policy Coordination Committee
CWG	Continuity Working Group
DHS	Department of Homeland Security
DOD	Department of Defense
ECG	Enduring Constitutional Government
ERG	Emergency Relocation Group
ESF	Emergency Support Function
FCD	Federal Continuity Directive
FE	Functional Exercise
FEA	Federal Executive Association
FEB	Federal Executive Board
FEMA	Federal Emergency Management Agency
FOC	FEMA Operations Center
FSE	Full-Scale Exercise
GAO	Government Accountability Office
GCC	Government Coordinating Council
GSA	General Services Administration
HQ	Headquarters
HSAS	Homeland Security Advisory System
HSEEP	Homeland Security Exercise and Evaluation Program
HSPD	Homeland Security Presidential Directive
IAB	Interagency Board
IT	Information Technology
MEF	Mission Essential Function

MOA/MOU	Memorandum of Agreement/Memorandum of Understanding
NCC	National Continuity Coordinator
NCR	National Capital Region
NCS	National Communications System
NEF	National Essential Function
NEP	National Exercise Program
NFG	Non-Federal Governments
NICC	National Infrastructure Coordinating Center
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NOC	National Operations Center
NRF	National Response Framework
NSPD	National Security Presidential Directive
OEP	Occupant Emergency Plan
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSTP	Office of Science and Technology Policy
PMEF	Primary Mission Essential Function
POC	Point of Contact
RRS	Readiness Reporting System
SCC	Sector Coordinating Council
TT&E	Test, Training, and Exercise
TTX	Tabletop Exercise
WMD	Weapons of Mass Destruction

ANNEX P. GLOSSARY

Activation – Once a continuity plan has been implemented, whether in whole or in part, it is considered “activated.”

Agencies – Federal departments and agencies means those executive departments enumerated in 5 U.S.C. § 101, together with 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 (USPS). The departments, agencies, and independent organizations are referred to in this document as “agencies.”

Agency head – The highest-ranking official of the primary occupant agency, or a successor or designee who has been selected by that official.

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 facilities – Locations, other than the primary facility, used to carry out essential functions, particularly in a continuity event. “Alternate facilities” refers to not only other locations, but also nontraditional options such as working at home (“teleworking”), telecommuting, and mobile-office concepts.

Automated data processing (ADP) equipment – Equipment that performs data processing largely by automatic means.

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, 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 the U.S. population, infrastructure, environment, economy, or government functions.

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

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 agencies, State, local, territorial, and tribal governments, and the private sector) as necessary to perform their Mission Essential Functions (MEFs).

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

Continuity capability – The ability of an organization to continue to perform its essential functions, using Continuity of Operations (COOP) and Continuity of Government (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 National Essential Functions (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 departments and agencies can execute their Primary Mission Essential Functions and Mission Essential Functions in support of National Essential Functions and continuity requirements under all circumstances.

Continuity Coordinators – Representatives of executive branch departments and agencies at the assistant secretary (or equivalent) level.

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. Note, this term may also be applied to non-Federal governments.

Continuity of Government Readiness Condition (COGCON) – COGCON is a system for establishing, measuring, and reporting the readiness of executive branch continuity programs, which is independent of other Federal Government readiness systems. (See Table 3 in Annex N for a detailed COGCON matrix.)

Continuity of Operations (COOP) – An effort within individual agencies to ensure they can continue to perform their Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs) during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.

Continuity Personnel - Those personnel, both senior and core, who provide the leadership advice, recommendations, and functional support necessary to continue essential operations

Continuity Policy Coordination Committee (CPCC) – A committee led by HSC 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; the Federal Emergency Management Agency; 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. The CAP System is a web-based tool that enables Federal, State, and local emergency response and homeland security officials to develop, prioritize, track, and analyze corrective actions following exercises or real world incidents. Users may enter data from a finalized After Action Report/Improvement Plan, track the progress of corrective action implementation, and analyze and report on trends in improvement plans.

Critical Infrastructure and Key Resources (CI/KR)– An interdependent network of vital physical and information facilities, networks, and assets, including the telecommunications, energy, financial services, water, and transportation sectors, that private business and the Government rely upon (including for the defense and national security of the United States). Critical infrastructures are those systems and assets so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security (including national economic security) and/or national public health or safety.

Delegation of authority – Identification, by position, of the authorities for making policy determinations and decisions at HQ, 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 – The capability to transfer statutory authority and responsibility for essential functions from an agency’s primary operating staff and facilities to other agency employees and facilities, and to sustain that operational capability for an extended period.

Drive-away kit – A kit prepared by, and for, an individual who expects to deploy to an alternate location during an emergency. The kit contains items needed to minimally satisfy an individual’s personal and professional needs during deployment.

Emergency operating records – Records that support the execution of an agency’s essential functions.

Emergency relocation group (ERG) – Pre-designated staff who move to an alternate facility to continue essential functions in the event that their normal work locations are threatened or have been incapacitated by an incident.

ERG member – A person who has been assigned responsibility to report to an alternate facility, as required to perform agency essential functions or other tasks related to continuity operations.

Emergency Support Function (ESF) – From the National Response Plan (NRP), a grouping of government and certain private sector capabilities into an organizational structure to provide support, resources, and services. The NRP groups functions as follows:

ESF #1	Transportation
ESF #2	Communications
ESF #3	Public Works and Engineering
ESF #4	Firefighting
ESF #5	Emergency Management
ESF #6	Mass Care, Housing, and Human Services
ESF #7	Resource Support
ESF #8	Public Health and Medical Services
ESF #9	Urban Search and Rescue
ESF #10	Oil and Hazardous Materials Response
ESF #11	Agriculture and Natural Resources
ESF #12	Energy
ESF #13	Public Safety and Security
ESF #14	Long-Term Community Recovery and Mitigation
ESF #15	External Affairs

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 – The critical activities performed by organizations, especially after a disruption of normal activities. There are three categories of essential functions: NEFs, PMEFs, and MEFs.

Executive departments and agencies – Executive departments enumerated in 5 U.S.C. 101, along with DHS, independent establishments as defined by 5 U.S.C. § 104(1), Government corporations as defined by 5U.S.C. § 103(1), and the United States Postal Service.

Facilities – Locations where an organization’s leadership and staff operate. Leadership and staff may be co-located in one facility or dispersed across many locations and connected by communications systems. Facilities must be able to provide staff with survivable protection and must enable continued and endurable operations.

Federal Continuity Directive (FCD) – A document developed and promulgated by DHS, in coordination with the CAG and in consultation with the CPCC, which directs

executive branch departments and agencies to carry out identified continuity planning requirements and assessment criteria.

Federal Executive Associations (FEAs) – A forum, modeled after but independent of the Federal Executive Boards, for communication and collaboration among Federal agencies outside of Washington, DC, utilized to help coordinate the field activities of Federal departments and agencies in localized sections of the Nation.

Federal Executive Boards (FEBs) – A forum, established by Presidential Directive in 1961, for communication and collaboration among Federal agencies outside of Washington, DC, utilized to help coordinate the field activities of Federal departments and agencies primarily in our Nation’s larger cities. With approximately 88% of all Federal employees working outside of the National Capital Region, the national network of 28 FEBs serves as a cornerstone for strategic partnerships 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.

Full-Scale Exercise – A full-scale exercise is a multi-agency, multi-jurisdictional, multi-discipline exercise involving functional (e.g., joint field office, emergency operations centers) and "boots on the ground" response (e.g., continuity staff relocating to their alternate sites to conduct scenario driven essential functions).

Functional Exercise – A functional exercise examines and/or validates the coordination, command, and control between various multi-agency coordination centers (e.g., emergency operations centers, joint field office). A functional exercise does not involve any "boots on the ground" (i.e., first responders or emergency officials responding to an incident in real time).

Government Functions – Government functions include both the collective functions of the heads of agencies as defined by statute, regulations, presidential direction, or other legal authority, and the functions of the legislative and judicial branches.

Homeland Security Advisory System (HSAS)– A series of tools used by DHS that provide the public with guidance on the status of the Nation’s homeland security. The system combines threat information with vulnerability assessments, and communicates this information to public safety officials and the public. The system includes Homeland Security Threat Advisories, Homeland Security Information Bulletins, and the Threat Level System.

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 (NEP) uses the HSEEP as a common methodology for exercises. The HSEEP also provides tools and resources to facilitate the management of self-sustaining homeland security exercise programs.

Hot Site –An alternate 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 (IAB) – A working group established by the NCC to review and recommend validation of potential PMEFs submitted by agencies for submission to the NCC for final approval.

Interoperability – “Interoperability” has two meanings: (1) The ability of systems, personnel, or agencies to provide services to and accept services from other systems, personnel, or agencies, 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 agencies, 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.

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

Mission Essential Functions (MEFs) – The limited set of agency-level Government functions that must be continued throughout, or resumed rapidly after, a disruption of normal activities.

Multiyear strategy and program management plan – A process that ensures the maintenance and continued viability of continuity plans.

National Communications System (NCS) – A system governed by Executive Order 12472 and comprised of the telecommunications assets of 24 Departments and Agencies. DHS serves as the Executive Agent for the NCS, which is responsible for assisting the President, the National Security Council, the Director of OSTP, 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 Policy – It is the policy of the United States to maintain a comprehensive and effective continuity capability composed of Continuity of Operations and Continuity of Government 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 the President and the Nation’s leadership will focus on to lead and sustain the Nation during a catastrophic emergency; NEFs, therefore, must be supported by COOP and COG capabilities.

National Exercise Program (NEP) – The NEP is the Nation’s overarching exercise program formulated by the National Security Council / Homeland Security Council (NSC/HSC), and executed by the Federal Interagency. All interagency partners have adopted HSEEP as the methodology for all exercises that will be conducted as part of the NEP.

National Incident Management System (NIMS) – HSPD-5 directed the Secretary of Homeland Security to develop and administer a NIMS to integrate effective practices in emergency preparedness and response into a comprehensive national framework for incident management. The NIMS will enable responders at all levels to work together more effectively to manage domestic incidents no matter what their cause, size, or complexity. The benefits of the NIMS include a unified approach to incident management, standardized command and management structures, and an emphasis on preparedness, mutual aid, and resource management.

National Infrastructure Coordinating Center (NICC) – A DHS entity, which operates 24 hours a day, seven days a week, to maintain operational and situational awareness of the Nation’s critical infrastructure and key resources and to provide a process and mechanism for coordination and information sharing with government and industry partners.

National Infrastructure Protection Plan (NIPP) – Pursuant to HSPD-7, the NIPP provides a coordinated approach to critical infrastructure and key resources (CI/KR) protection roles and responsibilities for Federal, State, local, tribal, and private sector security partners. The NIPP sets national priorities, goals, and requirements for effective distribution of funding and resources which will help ensure that our government, economy, and public services continue in the event of a terrorist attack or other disaster. The plan is based on the following:

- Strong public-private partnerships which will foster relationships and facilitate coordination within and across CI/KR sectors.
- Robust multi-directional information sharing which will enhance the ability to assess risks, make prudent security investments, and take protective action.

Risk management framework establishing processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk.

National Operations Center (NOC) – A DHS entity, which operates 24 hours a day, seven days a week, which is the primary national level hub for domestic situational awareness, common operational picture, information fusion, information sharing, communications, and coordination pertaining to the prevention of terrorist attacks and domestic incident management. The NOC is responsible for collecting and fusing

information from Federal, State, territorial, tribal, local, and private sector agencies. Information on domestic incident management is shared with Emergency Operations Centers at all levels through the Homeland Security Information Network.

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.

National Response Framework (NRF) – A guide for conducting comprehensive, national, all-hazards incident management. The NRF incorporates public and private sector participation at all levels, from Federal agencies to the State and community level, and also emphasizes the importance of personal preparedness by individuals and their families.

Occupant Emergency Plan (OEP) – A short-term emergency response program that establishes procedures for safeguarding lives and property.

Orders of succession – Provisions for the assumption of senior agency offices during an emergency in the event that any of those officials are unavailable to execute their legal duties.

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.

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.

Primary Mission Essential Functions (PMEFs) – Those department and agency Mission Essential Functions, 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.

Readiness Reporting System (RRS) – Department of Homeland Security program to collect and manage continuity capability data and assessments of executive branch departments and agencies and their status to perform their Priority Mission Essential Functions (PMEFs) in support of the National Essential Functions (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 agency personnel resume normal agency 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.

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 – The process by which risks are identified and evaluated.

Risk assessment – The identification and assessment of hazards.

Risk management – The process of identifying, controlling, and minimizing the impact of events whose consequences are or may be unknown, or events that are themselves fraught with uncertainty.

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

Tabletop Exercise (TTX) – A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting.

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 – The ability to work at a location other than the official duty station to perform work or emergency duties. This may include, but is not limited to, using portable computers, personal computers, high-speed telecommunications links, and mobile communications devices.

Test, training, and exercise (TT&E) – Measures to ensure that an agency's continuity plan is capable of supporting the continued execution of the agency's essential functions throughout the duration of a continuity event.

Virtual offices – An environment where employees are not collocated and rely exclusively on information technologies to interact and conduct their work across distance from multiple geographic locations.

Vital records – Electronic and hardcopy documents, references, and records to support essential functions during a continuity event. The two basic categories of vital records are (1) emergency operating records and (2) rights and interests records.

Warm Site – An alternate 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 (WMDs) – Weapons that are capable of killing a lot of 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. WMDs are generally considered to be nuclear, biological, chemical, and radiological devices, but WMDs can also be high-explosive devices.

Work-at-home – When employees carry out their work duties at their residence rather than their official duty station.

ANNEX Q. AUTHORITIES AND REFERENCES

The following are the authorities and references for this FCD.

AUTHORITIES:

- 1) The National Security Act of 1947 (50 U.S.C. § 404), July 26, 1947.
- 2) Homeland Security Act of 2002 (6 U.S.C. § 101 *et seq.*), November 25, 2002.
- 3) Executive Order 12148, *Federal Emergency Management*, July 20, 1979, as amended.
- 4) Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, April 3, 1984, as amended.
- 5) Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities*, November 18, 1988, as amended.
- 6) Executive Order 13286, *Establishing the Office of Homeland Security*, February 28, 2003.
- 7) National Security Presidential Directive 51/Homeland Security Presidential Directive 20, *National Continuity Policy*, May 9, 2007.
- 8) Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- 9) Homeland Security Presidential Directive 8, *National Preparedness*, December 17, 2003.
- 10) National Continuity Policy Implementation Plan, August 2007.
- 11) National Communications System Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, July 25, 2007.

REFERENCES:

- 1) 36 Code of Federal Regulations, Part 1236, *Management of Vital Records*.
- 2) 41 Code of Federal Regulations 101.20.103-4, *Occupant Emergency Program*.
- 3) Presidential Decision Directive 62, *Protection Against Unconventional Threats to the Homeland and Americans Overseas*, May 22, 1998.
- 4) Homeland Security Presidential Directive 1, *Organization and Operation of the Homeland Security Council*, October 29, 2001.
- 5) Homeland Security Presidential Directive 3, *Homeland Security Advisory System*, March 11, 2002.
- 6) Homeland Security Presidential Directive 5, *Management of Domestic Incidents*, February 28, 2003.
- 7) Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.

- 8) National Infrastructure Protection Plan, January 2006.
- 9) National Strategy for Pandemic Influenza, November 1, 2005.
- 10) National Strategy for Pandemic Influenza Implementation Plan, May 2006.
- 11) National Exercise Program Implementation Plan, April 2007.
- 12) National Incident Management System (NIMS), March 1, 2004.
- 13) NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.
- 14) NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, December 2006.
- 15) NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs, 2007 Edition.