NATIONAL CONTINUITY POLICY IMPLEMENTATION PLAN

Homeland Security Council

August 2007

NATIONAL CONTINUITY POLICY IMPLEMENTATION PLAN

Homeland Security Council

August 2007

THE WHITE HOUSE
WASHINGTON

My fellow Americans,

On May 4, 2007, I issued the *National Continuity Policy*, an updated, integrated approach to maintaining a comprehensive and effective continuity capability to ensure the preservation of our constitutional form of government and the continuing performance of National Essential Functions under all conditions.

Ours is a Nation of laws, engaged in a war against terror. We recognize, and must prepare for, the possibility of unforeseen events, natural disasters, and acts of terror. We must be prepared as a Nation, as a Federal Government, and as individual citizens to preserve, protect, and defend our way of life.

This *National Continuity Policy Implementation Plan* builds upon the *National Continuity Policy* and provides 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. This *Implementation Plan* also seeks to ensure that our Nation's efforts and resources will be brought to bear in a coordinated manner through integrated Continuity of Operations and Continuity of Government programs interwoven into routine, daily government operations. This *Implementation Plan* directs more than 75 critical actions, many of which have been initiated already, to ensure the effectiveness and survivability of our national continuity capability through any circumstance.

This *Implementation Plan* also articulates a recommitment of focus in the executive branch and highlights the importance of our partnership with the other branches of the Federal Government, other levels of government, and the private sector.

Working together, we will continue to prepare our Nation to confront the challenges of tomorrow.

GEORGE W. BUSH
THE WHITE HOUSE
AUGUST 2007

National Essential Functions

1. Ensuring the continued functioning of our form of government under the Constitution, including the functioning of the three separate branches of government;

2. Providing leadership visible to the Nation and the world and maintaining the trust and confidence of the American people;

3. Defending the 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;

4. Maintaining and fostering effective relationships with foreign nations;

5. Protecting against threats to the homeland and bringing to justice perpetrators of crimes or attacks against the United States or its people, property, or interests;

6. Providing rapid and effective response to and recovery from the domestic consequences of an attack or other incident;

7. Protecting and stabilizing the Nation's economy and ensuring public confidence in its financial systems; and

8. Providing for critical Federal Government services that address the national health, safety, and welfare needs of the United States.

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....ix

CHAPTER 1 – BACKGROUND AND OVERVIEW.....1
INTRODUCTION.....1
KEY CONSIDERATIONS AND CONCEPT OF OPERATIONS.....4
ROLES AND RESPONSIBILITIES.....12
SUMMARY.....14

CHAPTER 2 – NATIONAL PRIORITIES
INTRODUCTION.....15
KEY CONSIDERATIONS.....15
NATIONAL ESSENTIAL FUNCTIONS.....17
MISSION ESSENTIAL FUNCTIONS.....18
PRIMARY MISSION ESSENTIAL FUNCTIONS.....20
ROLES, RESPONSIBILITIES, AND ACTIONS.....22

CHAPTER 3 – CONTINUITY READINESS PROCEDURES AND METRICS.....27
INTRODUCTION.....27
KEY CONSIDERATIONS.....27
ROLES, RESPONSIBILITIES, AND ACTIONS.....31

CHAPTER 4 – COORDINATION, COMMUNICATION, AND INTEGRATION.....39
INTRODUCTION.....39
A. THE BRANCHES OF THE FEDERAL GOVERNMENT.....41
INTRODUCTION.....41
KEY CONSIDERATIONS.....41
ROLES AND RESPONSIBILITIES.....41
ACTIONS AND EXPECTATIONS.....42
B. FEDERAL, STATE, LOCAL, TERRITORIAL, AND TRIBAL GOVERNMENTS.....43
INTRODUCTION.....43
KEY CONSIDERATIONS.....43
ROLES AND RESPONSIBILITIES.....43
ACTIONS AND EXPECTATIONS.....45
C. PRIVATE SECTOR CRITICAL INFRASTRUCTURE OWNERS AND OPERATORS AND THE GOVERNMENT.....47
INTRODUCTION.....47
KEY CONSIDERATIONS.....47
ROLES AND RESPONSIBILITIES.....47
ACTIONS AND EXPECTATIONS.....47

APPENDIX A – NATIONAL SECURITY PRESIDENTIAL DIRECTIVE-51 (NSPD-51) / HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-20 (HSPD-20)....50

APPENDIX B – LIST OF DEPARTMENT AND AGENCY CATEGORIES (ANNEX A TO NSPD-51/HSPD-20) 56

APPENDIX C – GLOSSARY OF TERMS....57
ACRONYMS....57
DEFINITION OF TERMS....60

APPENDIX D – COGCON MATRIX....68

APPENDIX E – SELECTED CONTINUITY AUTHORITIES....70

APPENDIX F – CONTINUITY REQUIREMENTS AND METRICS....74

APPENDIX G – IMPLEMENTATION PLAN REQUIREMENTS AND DEADLINES MATRIX....76

APPENDIX H – MEF/PMEF IDENTIFICATION TIMELINE....82

Executive Summary

On May 4, 2007, the President issued the *National Continuity Policy ("Policy")* in National Security Presidential Directive-51/Homeland Security Presidential Directive-20 (NSPD-51/HSPD-20), which sets forth a new vision to ensure the continuity of our government. The President directed that:

> "**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.**"

In order to implement this *Policy*, government and private sector leaders should understand (1) the history, importance, and key components of our continuity program; (2) the importance of our key partners and the necessity to identify and ensure the continued execution of our Nation's Essential Functions; (3) the procedures to obtain metrics by which to measure our Nation's continuity capability and readiness; and (4) the coordination, communication, and integration among the three branches of the Federal Government, among all levels of government, and between government entities and the private sector.

This *National Continuity Policy Implementation Plan ("Plan")* was directed by the President to be the means by which the *Policy* is translated into action and is intended to be a **comprehensive and integrated list of directives for the Federal executive branch** in order to ensure the effectiveness and survivability of our national continuity capability. It is also an **educational primer** for those unfamiliar with continuity. While each chapter can be read independently for readers interested in a particular component of continuity, the entire *Plan* represents a **comprehensive source for current continuity resources and direction**.

Regardless of what it is called, 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.

While some of the details relating to the execution of particular Federal Government continuity programs are classified, the unclassified *Policy* makes clear that continuity planning for execution of Federal executive branch Essential Functions must be integrated into daily operations, functions, plans, and mission areas.

Therefore **this *Plan* directs that continuity planning occur simultaneously with the development of Federal department and agency programs**. This means that organizations must incorporate redundancy and resiliency as a means *and* an end. This *Plan* provides the guidance and direction necessary to achieve that result and identifies how the Federal executive branch will utilize thorough preparation and a continuous Continuity Program Management Cycle to analyze and execute programs, policies, and procedures to ensure continuity.

Chapter 1 – Background and Overview

In order to understand the new *Policy*, a continuity foundation must be laid that describes the history of Federal executive branch continuity programs and articulates the President's direction that the executive branch reorient itself and utilize an integrated, overlapping national continuity concept. This new continuity vision will significantly enhance our preparedness and ability to ensure the preservation of government and the continuation of essential functions. This chapter articulates goals and objectives and a continuity concept of operations to fulfill the President's vision. The continuous performance of essential functions must be supported with the right people, the

right resources, and the right planning. An organization's continuity capability—its ability to perform its essential functions continuously—rests upon key components or pillars built from the foundation of continuity planning and continuity program management. Upon this foundation four key continuity pillars must be built that represent the following:

- Leadership;
- Staff;
- Communications; and
- Facilities.

All of those elements are important during normal operating status and become critical during times of crisis. Because an organization's resiliency is directly related to its continuity capability, all organizations can improve their capability by developing a continuity concept of operations, which is further described in the chapter.

Chapter 2 – National Priorities

The goal of continuity in the executive branch is the continuation of National Essential Functions (NEFs), which are the critical responsibilities of the Federal Government to lead and sustain the Nation. The NEFs serve as the primary focus of Federal Government leadership during and in the aftermath of an emergency. In order to meet that goal, the objective for executive branch departments and agencies is to identify their respective Mission Essential Functions (MEFs) and Primary Mission Essential Functions (PMEFs) and ensure that those functions can be continued. The Federal Government's ability to successfully execute its NEFs successfully at all times, and especially during a crisis, is not an independent capability. The Federal Government relies upon key partners at all levels of government and in the private sector.

This *Plan* details a process for departments and agencies to identify their MEFs and PMEFs and ensure that they can be continued throughout, or resumed rapidly after, a disruption of normal activities. It further defines the roles, functions, and action items of the Nation's senior continuity officials, including the following:

- The National Continuity Coordinator (NCC) is responsible for coordinating, without exercising directive authority, the development and implementation of continuity *policy* for executive departments and agencies;
- The Secretary of Homeland Security serves as the President's lead agent for coordinating continuity *operations* and *activities*; and
- Continuity Coordinators at each executive department and agency are senior accountable officials at the Assistant Secretary (or equivalent) level responsible to work with their department or agency head to ensure effectiveness and survivability of the organization's continuity capability.

Chapter 3 – Continuity Readiness Procedures and Metrics

The government's ability to execute all of its continuity programs depends on a standardized but flexible set of operating procedures, resources to meet requirements, and performance measures to assess capabilities, recommend changes, and make improvements. This chapter articulates continuity readiness procedures and provides continuity metrics and requirements for executive departments and agencies to adopt. Some specific requirements include the following:

- A standardized Continuity Program Management Cycle to ensure consistency across continuity plans, establish consistent performance metrics, prioritize implementation plans, promulgate best practices, and facilitate consistent cross-agency continuity evaluations;
- A reporting requirement that department and agency heads certify their continuity capability to the NCC;
- A requirement that funding requests for continuity programs based on continuity requirements be included and prioritized appropriately within agency budget re-

quests submitted to the Office of Management and Budget (OMB);
- Regular assessments of continuity capabilities by DHS, which will be submitted to the NCC; and
- Monitoring by the Director of OMB of the progress in the execution of this *Plan* and reconciliation of prioritized funding requests with performance data and assessments.

Chapter 4 – Coordination, Communication, and Integration

The continuation of our constitutional form of government, the National Essential Functions, and support to the public in a catastrophic emergency are critically dependent on the effective functioning of all three branches of the Federal Government (legislative, executive, and judicial); the State, local, territorial, and tribal government structures; and key private sector entities. The identification of government and key private sector roles and the integration of their capabilities are vital to the Federal Government's overall continuity capability. This chapter discusses the coordination, communication, and integration necessary across all levels of government and with private sector critical infrastructure owners and operators. The chapter contains the following three sections addressing coordination, communication, and integration:

- Among the three branches of the Federal Government;
- Among Federal, State, local, territorial, and tribal governments; and
- Between private sector critical infrastructure owners and operators and the government.

The chapter recognizes the following key elements of interoperability:

- A cooperative effort among the legislative, executive, and judicial branches of the Federal Government is essential to preserve the constitutional framework under which the Nation is governed;
- By continuing the performance of essential functions through a catastrophic emergency, the State, local, territorial, and tribal governments support the ability of the Federal Government to perform NEFs, continue functioning within its constitutional form of government, and ensure that essential services are provided to the Nation's citizens; and
- Private Sector Critical Infrastructure Owners and Operators have a unique and invaluable role in ensuring the performance of essential functions during a catastrophic emergency.

Because the integration and coordination discussed in Chapter 4 is so vital, the *Plan* directs Federal executive departments and agencies to assist and coordinate with these key partners where appropriate. Additionally, the chapter explains how the President's continuity vision found in the *Policy* is made relevant to key partners and suggests implementation measures that should be taken to ensure that services are continued, law and order is maintained, and the principles of our Constitution survive.

Appendix

Included with the *Plan* are eight appended documents that provide additional reference material, timelines for implementation, and other information that will help continuity planners develop department and agency continuity plans.

National Continuity Policy Implementation Plan

Overarching Goals:

(1) **To educate** readers on the *National Continuity Policy* and the basic concepts of our continuity capability to ensure the preservation of our form of government under the Constitution and the continuing performance of National Essential Functions under all conditions;

(2) **To develop** a comprehensive and integrated list of assignments for the Federal executive branch; and

(3) **To provide** a comprehensive source for current continuity resources and direction.

Goals and Objectives:

- Goal #1 – To understand the transformation of continuity.
  - **Objective 1A** – To understand the history of continuity and the President's vision.
  - **Objective 1B** – To understand our Nation's continuity concept of operations and key considerations.
  - **Objective 1C** – To understand continuity roles and responsibilities.
- Goal #2 – To establish and ensure continuity of national priorities.
  - **Objective 2A** – To identify continuity partners and functions.
  - **Objective 2B** – To identify Mission Essential Functions.
  - **Objective 2C** – To identify Primary Mission Essential Functions.
  - **Objective 2D** – To establish roles, responsibilities, and actions for the Nation's senior continuity officials.
- Goal #3 – To ensure continuity readiness procedures and metrics.
  - **Objective 3A** – To establish a Continuity Program Management Cycle.
  - **Objective 3B** – To establish continuity requirements and metrics.
  - **Objective 3C** – To establish roles, responsibilities, and actions for continuity officials.
- Goal #4 – To promote interoperability.
  - **Objective 4A** – To promote interoperability among the branches of the Federal Government.
  - **Objective 4B** – To promote interoperability among Federal, State, local, territorial, and tribal governments.
  - **Objective 4C** – To promote interoperability between the private sector critical infrastructure owners and operators and the government.

GOAL #1 To understand the transformation of continuity.

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.

– *National Security Presidential Directive-51/Homeland Security Presidential Directive-20 (NSPD-51/HSPD-20) of May 4, 2007*

OBJECTIVE 1A – To understand the history of continuity and the President's vision.

INTRODUCTION

The *National Continuity Policy ("Policy")* of the United States is designed to ensure an uninterrupted succession of our constitutional form of government in the face of any hazard, recognizing that catastrophic incidents could pose a threat to our citizens and our way of life. The importance of continuity at the national level is embodied in our responsibility to preserve our constitutional form of government. The Constitution is the bedrock of our system of laws and individual rights and provides the basis for governance and leadership. The protection and continuance of our form of government is also critical to government systems at the State and local levels. The services provided by governments at all levels and the private sector affect the everyday lives of citizens and customers. Many of those services are essential, particularly in the areas of law and order, health, and daily sustenance. Thus, our constitutional form of government embodies governance at the highest level down to the rights, privileges, and services provided to individual citizens.

The *Policy* takes an all-hazards approach, emphasizing a comprehensive planning effort designed to accomplish the following: provide the capability to have continuity of leadership visible to the Nation and the world; defend the Nation against all enemies, foreign and domestic; maintain and foster relationships with other nations; protect against threats to the homeland; ensure the Nation's readiness to respond rapidly and effectively to the consequences of an attack or other incident; protect the Nation's economy and ensure public confidence in its financial systems; and provide critical Federal Government services that address the national health, safety, and welfare needs of the United States.

This chapter provides an understanding of the concept of continuity, its importance to our Nation's security and well-being, the components of a viable continuity program, and the responsibilities of key officials in the planning and execution of our continuity capability.

The concept of continuity for the Federal Government is not a new one. From the very beginning, the Federal Government has needed to plan for worst case scenarios to ensure that our form of government continues. In 1783 Congress faced several hundred members of the militia who surrounded Independence Hall in Philadelphia demanding back pay that they were owed and threatening our fragile pre-Constitution Nation. Ten years later, Congress had an opportunity to address another threat when Federal workers relocated away from the Nation's capital in Philadelphia as a result of the 1793 Yellow Fever epidemic and continued government business.

During the Cold War, the threat of nuclear attack from the Soviet Union prompted the establishment of programs and related facilities that would ensure the continuation of government functions. In the post-Cold War era, continuity planning began to recognize the danger of natural hazards and the terrorist threat to the continuation of government functions. In 1995, an Executive Office of the President memorandum advised Federal executive branch continuity planners to expand planning parameters to include natural disasters and terrorism, in addition to the continued nuclear threat. In 1998, Presidential Decision Directive-67 (PDD-67) ("Enduring Constitutional Government and Continuity of Government Operations") reaffirmed an all-hazards approach to continuity (i.e., preparation for all scenarios) and called for "continuity of operations" (defined below) to be the foundation of Federal Government continuity programs. PDD-67 emphasized the responsibility of executive branch departments and agencies to perform essential government functions under all conditions. *The all-hazards approach and importance of performing essential functions continues today.*

Historically the Federal Government has defined continuity efforts using the terms "COOP", "COG", and "ECG" *(see Box 1 below)*.

"COOP," or Continuity of Operations, is an effort within *individual* organizations (e.g., Federal executive branch departments and agencies) to ensure that Mission Essential Functions 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 National Essential Functions continue to be performed during a catastrophic emergency; and

"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 constitutional responsibilities and provide for orderly succession, appropriate transition of leadership, interoperability, and support of the National Essential Functions during a catastrophic emergency.

– Note: These are operational definitions provided to facilitate a better understanding.

Box 1

In the past, COOP, COG, and ECG plans and programs were separate, compartmented activities. However, the lessons we now have 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.

The old organizational framework has changed. Pursuant to NSPD-51/HSPD-20, and with this *National Continuity Policy Implementation Plan*, the **President directs the executive branch to reorient itself and to utilize an *integrated, overlapping national continuity concept* in order to ensure the preservation of our government and the continuing performance of essential functions**. *(See Figure 1.)*

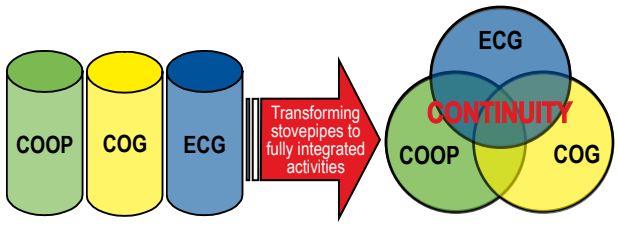


Figure 1

Continuity responsibility and planning is no longer a separate, compartmented function of an independent cell of a few planners in each government department and agency. In recent years, some departments and agencies have begun to integrate continuity planning into all aspects of their organization's mission, moving it from the "other duties as assigned" category to a function integrated across all groups within an organization and creating a culture of continuity. **This *Implementation Plan* directs that continuity planning occur simultaneously as functions are developed and executed.** This concept is reinforced by the directive in NSPD-51/HSPD-20 that each Federal executive branch department and agency head shall "appoint a senior accountable official, at the Assistant Secretary level, as the Continuity Coordinator for the department or agency." (The responsibilities for that official are described further in Chapter 2.)

While the Federal Government has invested significant resources to ensure the continuity of government operations during scenarios ranging from utility failures and natural disasters to nuclear, chemical, and/or biological attacks, it is critical to remember that most of the Federal Government's National Essential Functions (NEFs) prescribed in NSPD-51/HSPD-20 cannot be performed without the robust involvement of non-Federal Governments and the private sector. Some of those functions include public health, law enforcement, the administration of justice, economic stability, and response to natural and manmade disasters. While both large and small private sector companies have long understood the need for continuity planning and implementation, especially for financial reasons, government organizations have also had some continuity success stories. *(See Box 2 below for examples of events in August 2005 surrounding Hurricane Katrina, one of the deadliest and costliest hurricanes ever to hit the U.S.)*

- National Finance Center – Planning for continuity of operations enabled the National Finance Center (NFC) in New Orleans to pay more than half a million Federal workers on time while Hurricane Katrina was bearing down. NFC then made subsequent payrolls—its largest ever— without any delays. According to officials, NFC had gone through various diverse scenarios in disaster recovery planning and exercises as part of its preparedness for just such an event. There was a structured timeline for reviewing the continuity of operations plan every year, beginning with continuity of operations plan requirements and business impact analysis at the unit level. A NFC official said that key NFC staff members worked the weekend before landfall at the New Orleans facility to complete payroll processing for federal employees, and then shut down operations and deployed to backup locations before the hurricane hit New Orleans. NFC backup data was trucked out of the New Orleans facility. When Hurricane Katrina made landfall in Louisiana NFC had already sent an advance deployment team to its backup sites in Philadelphia, Pennsylvania, and Texas. That same night, the trucks arrived at an alternate processing facility outside Philadelphia. The backup tapes also enabled the New Orleans NFC staff to restore many operations within 2 days of the devastation. Within a 50-hour period, NFC had the data center recovered and began catch-up processing to bring applications up to current state.

- U. S. Coast Guard – The Coast Guard was able to mitigate some of the communication shortfalls it experienced, in part because of its planning assumption that "communications systems could be heavily damaged or destroyed" during a natural disaster. This assumption prompted Coast Guard officials to build into their contingency plans approaches that were not reliant on communication systems and that allowed personnel to act independently or with limited guidance from commanding officers. As a result of the contingency plan, personnel in charge of the assets knew their mission prior to the storm and did not need to communicate any further with district command to fulfill their operation. In addition, as planned, the Coast Guard pre-placed communication equipment before the storm. Members of the Coast Guard Auxiliary were notified prior to the hurricane's landfall and provided communication capabilities after the storm passed, which according to Coast Guard officials, was critical to conducting search and rescue operations.

- Social Security Administration – The Social Security Administration had enhanced planning and pre-established procedures in place to provide immediate emergency payments to the significant number of beneficiaries who evacuated and did not receive their monthly checks. With these procedures in place, the Social Security Administration had the capability to deploy staff and equipment from its 1,300 offices across the nation to address the increased workload.

– Source: GAO Report GAO-06-618 (September 2006)
- Catastrophic Disasters: Enhanced Leadership, Capabilities, and Accountability Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System

Box 2

OBJECTIVE 1B – To understand our Nation's continuity concept of operations and key considerations.

KEY CONSIDERATIONS AND CONCEPT OF OPERATIONS

The continuous performance of essential functions must be guaranteed with the right people, the right resources, and the right planning. Continuity cannot be an afterthought for organizations as they strive to perform essential functions.

Unfortunately, there are a myriad of natural hazards, manmade threats, and acts of war that are capable of interrupting the functions of government and private sector organizations. Some of these threats are more predictable than others. Hurricanes (e.g., Andrew, Hugo, and Katrina), ice storms, flooding, tornadoes, and pandemic outbreaks may or may not allow for a warning time prior to their arrival. Other hazards, such as earthquakes, accidents, sabotage, and terrorism, which are not as predictable, may occur suddenly and with little or no warning. We also continue to face the threat of a strategic nuclear attack, a chemical or biological attack, and "dirty bomb" radiological devices. All of those threats are real and dangerous, and they could adversely affect the ability of government at all levels and the private sector to provide essential functions and services to our citizens. Thus, we have a critical and ongoing need to ensure the effectiveness of our continuity capability through planning, operations, tests, training, and exercises.

Executive departments and agencies will incorporate the following key continuity concepts in developing specific operational procedures to ensure a robust continuity capability: an understanding of essential functions; consideration of risk management; clear lines of authority; necessary communications capability; adequate facilities; ample security; thoughtful

preparedness; and integration with incident management (as required). The consideration, preparation, and execution of those elements are fundamental for a successful concept of operations for continuity.

ESSENTIAL FUNCTIONS

The Federal executive branch prioritizes the following three categories of essential functions, which are further described in Chapter 2:

- **Mission Essential Functions (MEFs)** – The limited set of department and agency-level government functions that must be continued after a disruption of normal activities.
- **Primary Mission Essential Functions** (PMEFs) – A subset of department and agency MEFs that directly support the NEFs.
- **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 Federal executive branch recognizes that the entire spectrum of essential functions might 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 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. Directly linking PMEFs to a NEF requires the Federal executive departments and agencies to identify the most critical functions that must continue through an emergency and the planning required to perform those functions. This model serves as a template for other government organizations and for private sector entities.

KEY COMPONENTS

An organization's continuity capability—its ability to perform its essential functions continuously—rests upon key components or pillars, which are in turn built on the foundation of continuity planning and continuity program management. Those key pillars are Leadership, Staff, Communications, and Facilities *(see Figure 2 below)*. They are important during normal operating status, and they are critical during times of crisis, especially when an organization is functioning with limited information or resources. An organization's resiliency is directly related to its continuity capability.

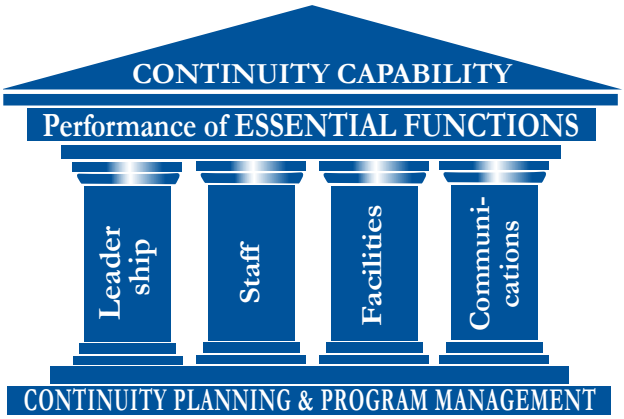


Figure 2

A resilient continuity capability includes the following concepts:

"**Continuity Capability**" is the ability of an organization to continue performance of essential functions, utilizing Continuity of Operations and Continuity of Government programs and integrated, day-to-day operations with a primary goal of ensuring the preservation of our form of government under the Constitution and the continuing performance of National Essential Functions under all conditions. Built from the foundation of continuity planning and continuity program management, the key pillars of continuity capability are Leadership, Staff, Communications, and Facilities.

"**Essential Functions**" are the critical activities that are performed by organizations.

"**Leadership**" comprises the senior decision-makers designated to head an organization (e.g., President, Cabinet Secretary, Governor, Chief Executive Officer, or manager). Ensuring survivable leadership is accomplished by physically protecting the person (sheltering in place or relocating away from the threat), as well as having a prioritized list of designated successors. The designation as a successor enables a person to act for and exercise the powers of the principal in the event of death, incapacity, or resignation.

"**Staff**" comprises those personnel that provide the leadership advice, recommendations, and the functional support necessary to continue essential operations.

"**Communications**" are voice, video, and data capabilities that enable leadership and staff to conduct Essential Functions. Robust communications help ensure that leadership receives coordinated, integrated policy and operational recommendations and enable coordination with Federal executive branch departments and agencies; State, local, territorial, and tribal governments; and the private sector as necessary to perform Essential Functions.

"**Facilities**" represent locations where leadership and staffs may operate. Leadership and staff may be co-located in one facility or dispersed through many locations, connected virtually through communications systems. Facilities must be able to provide survivable protection and enable continued, endurable operations.

"**Planning**," the first step in a robust Program Management Cycle, includes pre-identifying the right people, places, budgeting, resources, tasks, and procedures required to fulfill Essential Functions.

"**Program Management**" is the continuous cycle of planning, training, evaluating, and implementing corrective actions. (This is further discussed in Chapter 3.)

Note: These operational definitions are provided to facilitate a better understanding of Figure 2.

Box 3

Before and during an emergency situation that triggers a continuity plan, leaders and staff must be prepared to allocate scarce resources. Organizations must identify the people, communications, facilities, infrastructure, transportation, and funding needed to support continuity programs. Those programs must be integrated into the budget process at all levels.

Pillars 1 and 2: People – Leadership and Staff

People are the heart and soul of any organization and the most valuable resource it has. Choosing the right people for an organization's staff is always important, and this is especially true in a crisis situation. Leaders are needed to set priorities and keep focus.

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 departments and agencies, is important to reassure the Nation and give confidence to our citizens that the principal or appropriate successor is managing whatever crisis the Nation faces and ensuring the performance of our National Essential Functions.

For the Presidency, the Constitution and statute establish the Order of Presidential Succession for officials who meet the constitutional requirements as follows:

The Vice President	Secretary of Commerce
Speaker of the House	Secretary of Labor
President Pro Tempore of the Senate	Secretary of Health and Human Services
Secretary of State	Secretary of Housing and Urban Development
Secretary of the Treasury	Secretary of Transportation
Secretary of Defense	Secretary of Energy
Attorney General	Secretary of Education
Secretary of the Interior	Secretary of Veterans Affairs
Secretary of Agriculture	Secretary of Homeland Security

Box 4

Leaders and staff must be sufficiently trained to be able to perform their duties in a continuity environment (i.e., one in which an organization is faced with an interruption of normal operations for a potentially protracted period of time). In order 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 person 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 national continuity policy. Under NSPD-51/HSPD-20, all organizations must identify the communication requirements needed to perform their PMEFs 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 MEFs 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.

Daily operating facilities must be evaluated for "hardness" (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).

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 thinking through all of the requirements and procedures needed to perform Essential Functions and establishing contingency plans in the event that key resources are not available. Other planning components include budgeting, developing operational plans, and identifying clear goals and priorities.

Chapter 2 of this *Plan* discusses national priorities and the planning required for Executive Branch MEFs and PMEFs, including information about conducting a Business Process Analysis and a Business Impact Analysis.

Chapter 3 of this *Plan* discusses planning as the first step in a robust Continuity Program Management Cycle and details the rest of the continuous process to test, evaluate, and make corrective actions to continuity plans.

In addition to the planning elements listed above, continuity planning requirements also include consideration of risk management, geographic dispersion, security, preparedness, and integration of continuity and incident management.

- *Risk Management*

Risk management is the process to identify, control, and minimize the impact of uncertain events. While there are many well-documented methodologies for risk management—some are referred to as risk analysis—most require an assessment and understanding of three basic concepts:

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

When reviewing an organization's risks and risk management programs, additional factors such as probability, mission priorities, and impact assessments must be considered. Further, cost may also be a factor as 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 will never be fully mitigated, and no organization could afford to counter every threat to its mission. Intelligent analysis of where and when to focus resources and/or apply funding and other assets is critical for successful continuity planning.

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

Appropriate planning and investment to ensure survival from natural disasters and deliberate attack must go beyond classical risk analysis of "severity times probability." As an integral part of risk management, an organization's leaders must think beyond the internal effects of their inability to perform Mission Essential Functions. Department and agency heads and staff at all levels must consider the interdependencies between and among departments and agencies that share critical roles in the delivery of NEF capabilities.

- *Geographic Dispersion*

Incorporating geographic dispersal in an organization's normal daily operations, as appropri-

ate, can significantly enhance the organization's resilience and reduce the risk of losing the capability to perform essential functions. While some leadership and staff want to be located "close to the flagpole" (i.e., headquarters), organizations should appropriately disperse staff elements and functions away from the main headquarters building on a routine operating basis to enhance the survival of key personnel and functions. With the continuing improvements in desktop teleconferencing and collaborative tools, the ability to conduct daily business from geographically dispersed locations is growing more commonplace and, if done routinely, will serve as a model for dispersed operations in the event of an emergency. Geographic dispersion of leadership, data storage, personnel, and other capabilities may be essential to the performance of MEFs following a catastrophic event.

The US Department of Health and Human Services, which pays for about 40 percent of the Nation's healthcare, established multiple nodes of payment processing centers which were geographically dispersed to ensure uninterrupted capability. Each node maintains the capability to assume the responsibilities of the other payment centers.

Box 5

- *Security*

Security is a key element to any continuity program to protect plans, personnel, facilities, and capabilities to prevent adversaries from interdicting your 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. Organizations must adopt appropriate security measures to protect information and capabilities while ensuring awareness of plans and procedures by leadership and staff to enable them to effectively function in an emergency.

Another key component of our homeland security is securing cyberspace. This is an ongoing, complex challenge that requires a coordinated and focused effort from the Federal Government, State and local governments, the private sector, and the American people. As identified by *The National Strategy to Secure Cyberspace*, our Nation's critical infrastructures consist of the physical and cyber assets of public and private institutions in several sectors: agriculture; food; water; public health; emergency services; government; defense industrial base; information and telecommunications; energy; transportation; banking and finance; chemicals and hazardous materials; and postal and shipping. Cyberspace is the nervous system of these infrastructures—the control system of our country. Cyberspace consists of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security.

- *Readiness and Preparedness*

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 before, during, and after an incident.

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

Four COGCON levels provide for an incremental increase in and deployment of people and

resources to enhance staffing, survivability, responsiveness, and availability of assets for immediate support to leadership. The designated COGCON level is based on the current threat and/or risk to the Federal Government.

- COGCON 4 is the day-to-day readiness level with Federal executive branch government employees at their normal work locations.

- COGCON 3 requires Federal executive branch departments and agencies to "warm up" their alternate sites and capabilities, which includes test ing communications and IT systems and ensuring alternate facilities are prepared to receive continuity staffs.

- COGCON 2 calls for a deployment of up to 50-75% of continuity staffs to relocate from their normal work sites to alternate locations, establish their ability to conduct operations, and prepare to perform their organization's essential functions in the event of a catastrophic emergency.

- COGCON 1 calls for a full deploy ment of designated leadership and continuity staffs to perform the organization's essential functions from alternate facilities either as a result of, or in preparation for, a catastrophic emergency.

The President or his designee determines and issues the COGCON level. The Federal Emergency Management Agency (FEMA) Operations Center (FOC) makes the appropriate notifications to executive branch departments and agencies, which shall comply with the requirements and assigned responsibilities documented in the COGCON system. While COGCON is an independent system, it is influenced by other alert systems such as the Department of Defense's (DOD) Defense Readiness Conditions (DEFCON), DOD's Force Protection Conditions (FPCON), and the Department of Homeland Security's (DHS) Homeland Security Advisory System (HSAS). (Appendix D includes a matrix with the various requirements and stages of COGCON for departments and agencies.)

Organizations may consider creating a "continuity readiness posture" similar to the executive branch's COGCON system.

While COGCON establishes the executive branch readiness levels, DHS uses several separate tools to enhance readiness and drive preparedness actions for the general public. The HSAS provides guidance to the public on the status of our homeland security. This System combines threat information with vulnerability assessments and communicates this information to public safety officials and the general public. Updates can be found at the Department website at ***www.dhs.gov***. The HSAS includes the following components:

- **Homeland Security Threat Advisories** contain actionable information about an incident involving, or a threat targeting, critical national networks or infrastructures or key assets. They could, for example, relay newly developed procedures that, when implemented, would significantly improve security or protection. They could also suggest a change in readiness posture, protective actions, or response. This category includes products formerly named alerts, advisories, and sector notifications. Advisories are targeted to Federal, State, and local governments, private sector organizations, and international partners

- **Homeland Security Information Bulletins** communicate information of interest to the Nation's critical infrastructures that do not meet the timeliness, specificity, or significance thresholds of Threat Advisories. Such information may include statistical

reports, periodic summaries, incident response or reporting guidelines, common vulnerabilities and patches, and configuration standards or tools. It also may include preliminary requests for information. Bulletins are targeted to Federal, State, and local governments, private sector organizations, and international partners.

- The **Threat Level System** is used to communicate with public safety officials and the public at-large through a threat-based, color-coded system so that protective measures can be implemented to reduce the likelihood or impact of an attack. Since raising the threat condition has economic, physical, and psychological effects on the Nation, the Homeland Security Advisory System can place specific geographic regions or industry sectors on a higher alert status than other regions or industries, based on specific threat information. *(See Figure 3.)*

Figure 3

Preparedness is a dynamic process involving identification of MEFs, risk management, planning, training, exercises, continual assessment of plans and capabilities, and remediation. The better prepared we are to deal with threats, the better our continuity capability will be.

Integration of Continuity and Incident Management

Integration of continuity planning with incident management planning and operations include responsibilities delineated in the National Response Plan (NRP) and is linked to an organization's ability to conduct its PMEFs. This *Implementation Plan* does not delineate new procedures for incident management activities other than already established protocols; however this *Plan* does emphasize that organizations with incident management responsibilities must incorporate requirements to perform these functions into continuity planning. Integration is especially key for interagency coordination groups that monitor or convene during an incident, such as the DHS National Operations Center (NOC), National Response Coordinating Center (NRCC), and National Infrastructure Coordinating Center (NICC); Joint Field Offices (JFOs); and Regional Response Coordination Centers (RRCC) to name a few. The lead agency for these interagency groups must develop and share continuity plans to ensure the group's continued capability regardless of circumstance.

OBJECTIVE 1C – To understand continuity roles and responsibilities.

ROLES AND RESPONSIBILITIES

Roles:

Federal Government

The National Continuity Coordinator (NCC) leads the development and coordinates the implementation of continuity policy. The Continuity Policy Coordination Committee, led by a designee of the NCC, is the main day-to-day forum for such policy coordination. The Secretary of Homeland Security is responsible for coordinating the implementation, execution, and assessment of continuity operations and activities of executive branch departments and agencies. Heads of executive departments and agencies are required to plan, program, and budget resources appropriate to their organization at levels that ensure their continuity capability to accomplish their essential functions. Additionally, heads of executive departments and agencies should partner with State, local, territorial, and tribal governments, as well as private sector owners and operators, to develop continuity plans that are consistent with Federal plans to the extent possible. That should be accomplished in coordination with the Secretary of Homeland Security, who is responsible for developing and promulgating continuity planning guidance and directives. The legislative and judicial branches develop and implement their own unique continuity programs and coordinate with the executive branch as appropriate to ensure ECG capability. (Chapter 4A of this *Plan* contains specific guidance for the legislative and judicial branches.)

State, Local, Territorial, and Tribal Governments

State, local, territorial, and tribal governments play an integral role in determining the needs of the general public and ensuring the continuation of essential services on a daily basis (e.g., police and fire services, road construction, and public education). Those non-Federal Government partners should work with DHS, with existing procedures, in coordinating continuity plans. Those processes facilitate the allocation of resources for the development of continuity plans and the procurement of emergency response equipment. In addition, Federal Executive Boards, and other officially designated entities, may also augment and strengthen those coordination efforts. Continuity planners at the Federal executive branch level should incorporate the capabilities of State, local, territorial, and tribal governments into their planning and exercise activities to the extent possible. (Chapter 4B of this *Plan* contains specific guidance for non-Federal Government entities.)

Private Sector

In addition to government functions, continuity of essential services provided by the private sector is also extremely important. Critical infrastructure protection is a shared responsibility among Federal, State, local, territorial, and tribal governments and the owners and operators of the Nation's critical infrastructure and key resources (CI/KR). Partnership between the public and private sectors is essential, in part because the private sector owns and operates 85% of the Nation's critical infrastructure while government agencies have access to critical threat information. Existing directives (e.g., Homeland Security Presidential Directive-7 of December 17, 2003, "Critical Infrastructure Identification, Prioritization, and Protection") provide guidance for critical infrastructure protection and should be included in continuity planning and utilized to the maximum extent. (Chapter 4C of this *Plan* contains specific guidance for the private sector.)

Continuity Planners

Continuity planners at all levels have the responsibility of fully understanding their organization and monitoring the direction, guidance, and best practices of government and the private sector in order to develop the

most relevant and robust continuity programs. Candid and honest assessments, appropriate application of risk management principles and concepts, and openness to new concepts and ideas—from maximizing the benefits of telework to planning for viable geographic dispersion of functions and leadership—are the underpinnings of an effective program. Maximizing the use of exercises, whether table-top or full scale, in order to test plans as well as to highlight areas for improvement, will further hone continuity plans. Continuity planners are integral parts of an organization and must be positioned at a level to be effective. **Continuity can no longer be "bolted on"—it must be built into all functions and mission areas.**

Individuals

The most basic and fundamental foundation of continuity, at any level of government or within the private sector, is personal responsibility and readiness. Individuals must understand their roles and responsibilities within their respective organizations. They need to know and be committed to their duties in a continuity environment. This may involve separation from family or other hardships in time of crisis. Some might be required to report to work at a primary or alternate site; others may be directed to remain at home for teleworking or to remain available for reach-back and staff augmentation. Individuals need to understand and be willing to perform in these situations to ensure an organization can continue its Essential Functions.

At the same time, most individuals will need to make sure that family members are taken care of in an emergency situation. DHS and the American Red Cross have provided excellent planning guides in a variety of educational documents and on websites such as *www.ready.gov.*

Responsibilities:

Continuity responsibilities are shared between those who develop policy and those charged with implementation of that policy. NSPD-51/HSPD-20 directs the NCC to coordinate the development and implementation of continuity policy for Federal executive branch departments and agencies.

In accordance with the direction and guidance provided by the NCC and the Secretary of Homeland Security, Federal departments and agencies are responsible for implementation of continuity policy.

All other Federal organizations, non-Federal Government entities (including State, local, territorial, and tribal governments) (NFGs), and private sector entities are encouraged to adopt policies and procedures consistent with NSPD-51/HSPD-20 and this *Implementation Plan*.

SUMMARY

Chapter 1 provides both a background on continuity and an overview of basic continuity concepts and requirements. The remainder of this *Implementation Plan* provides guidance and direction and, where appropriate, goals and milestones that must be met in order to implement the provisions of NSPD-51/HSPD-20. This *Plan* directs actions to be taken by the heads of Federal executive branch departments and agencies and is a useful reference document for non-Federal Government and private sector entities. It is also designed to foster and facilitate coordination and cooperation between the Federal executive branch and the legislative and judicial branches of government. The extent to which all organizations, public or private, speak the same language; share the same goals; and coordinate fully on continuity planning, training, exercising, and operations will determine this Nation's overall readiness and ability to perform operations in a crisis.

Continuity planning is simply the good business practice of ensuring the execution of essential functions and a fundamental duty of public and private entities responsible to their stakeholders.

Box 6

GOAL #2 **To establish and ensure continuity of national priorities.**

INTRODUCTION

The ultimate goal of continuity in the executive branch is the continuation of National Essential Functions (NEFs). In order to achieve that goal, the objective for executive departments and agencies is to identify their Mission Essential Functions (MEFs) and ensure that those functions can be continued throughout, or resumed rapidly after, a disruption of normal activities. While the Federal Government provides myriad services to the American people, it is important to identify those services that must be continued during an emergency. Setting priorities is difficult, but organizations should not wait for a crisis to determine what is important. This chapter defines the most important national priorities, directs executive departments and agencies to identify their most important functions, tasks the NCC to validate department and agency Primary Mission Essential Functions, and acknowledges the important partnership that the Federal Government has with other government entities and with private sector owners and operators.

KEY CONSIDERATIONS

OBJECTIVE 2A – To identify continuity partners and functions.

Partners

While this *Implementation Plan* is primarily directed at the executive branch of the Federal Government, continuity cannot occur without the commitment and dedication of many others who play integral roles in ensuring our homeland security.

Those partners include the following *(see Figure 4)*:

- 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

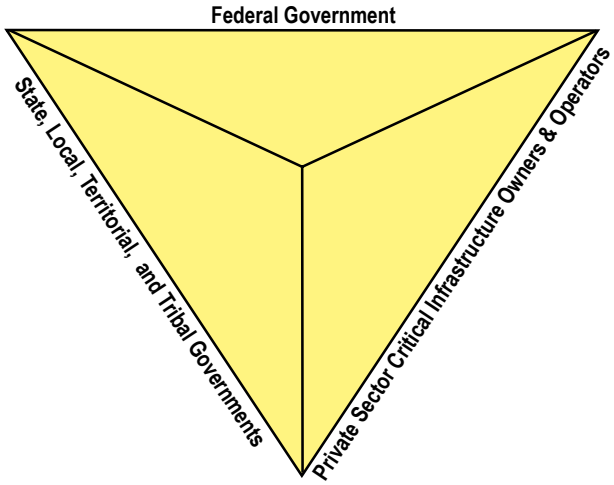


Figure 4

Functions

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

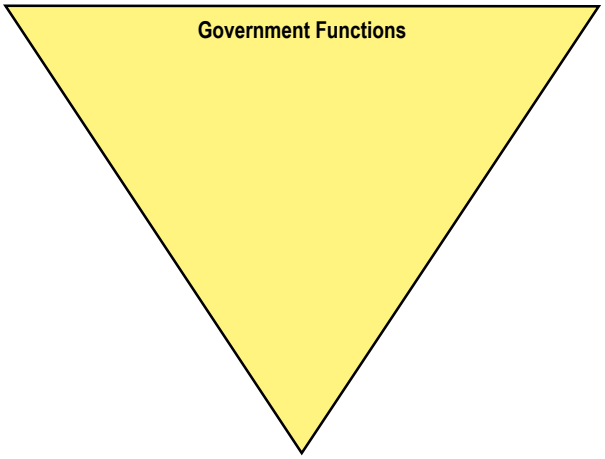


Figure 5

Mission Essential Functions (MEFs): **MEFs are described as the limited set of department- and agency-level government functions 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 general public, and sustain the industrial/economic base during disruption of normal operations. Once identified, MEFs serve as key continuity planning factors for departments and agencies to determine appropriate staffing, communications, information, facilities, training, and other requirements.

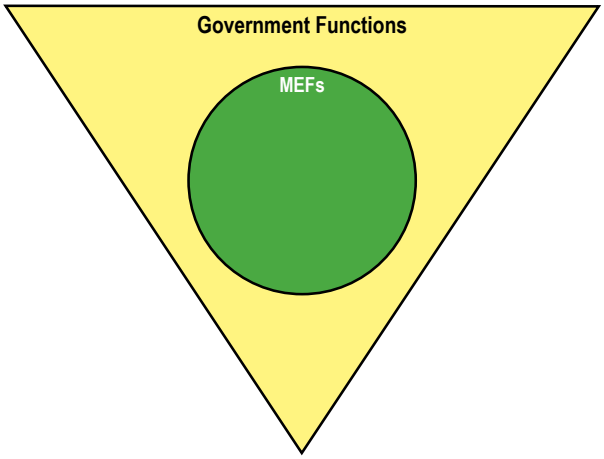


Figure 6

Primary Mission Essential Functions (PMEFs): **PMEFs are those department and agency mission essential functions, validated by the National Continuity Coordinator, which must be performed in order to support the performance of the NEFs before, during, and in the aftermath of an emergency.** 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.

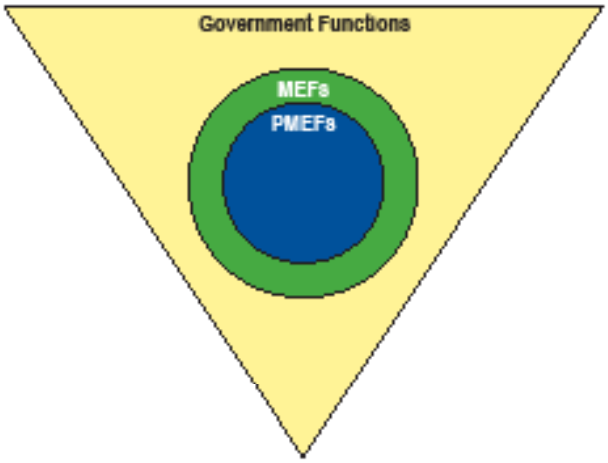


Figure 7

National Essential Functions (NEFs): In accordance with NSPD 51/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 leadership during and in the aftermath of an emergency.

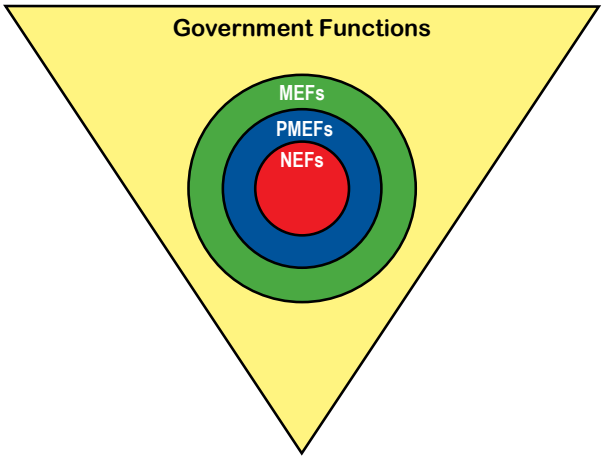


Figure 8

Figure 9 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.

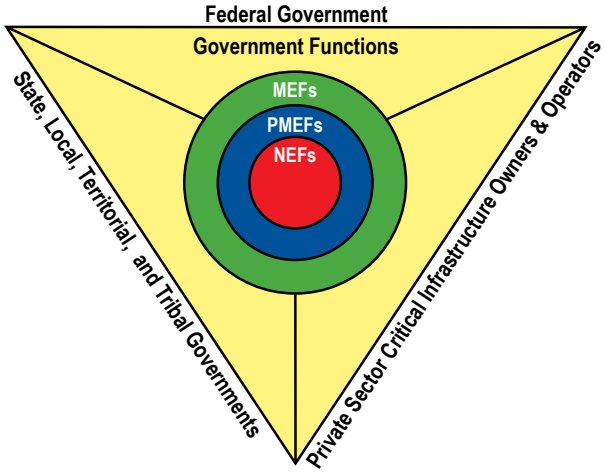


Figure 9

NATIONAL ESSENTIAL FUNCTIONS

The NEFs will be the primary focus of the President and the national leadership during and following an emergency. These are categories of functions performed by one or more departments and agencies; they are not new authorities, requirements, or functions. The National Essential Functions (NEFs) are:

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 response to and recovery from the domestic con-**

sequences 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.

MISSION ESSENTIAL FUNCTIONS

OBJECTIVE 2B – To identify Mission Essential Functions.

Process to Identify MEFs

Process – Prelude

Identifying department and agency Mission Essential Functions is a prerequisite for continuity because it establishes the parameters that drive the department and agency efforts in all other planning and preparedness areas. Identification of MEFs requires an objective review of department and agency functions that delineates those time-sensitive and/or critical activities that must be sustained in an emergency. In 2005, an effort began to identify PMEFs. This process is a refinement of early endeavors. Many of the PMEFs identified by departments and agencies in 2005 were actually part of the larger set of MEFs. Much of the process described in this document will build upon the previous effort to produce a more refined and synchronized set of MEFs and PMEFs.

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 determine that the function must be performed under all circumstances either uninterrupted, with minimal interruption, or requiring immediate execution in an emergency?	YES	NO
If the answer to one or both of these questions is "NO," the function is probably not a MEF.		

Box 7

Process – MEF Identification and Analysis

Departments and agencies will do the following when identifying and analyzing MEFs *(see diagram on page 19 for further details):*

- Review their organization's functions as directed by applicable law, presidential directives, executive orders, and other executive branch directives to identify their MEFs;
- Conduct an MEF Business Process Analysis (BPA) to identify and map functional processes, workflows, activities, personnel expertise, systems, data, and facilities inherent to the execution of each identified MEF (i.e., define how each MEF is performed and executed with a business process flow map), which must be performed under all circumstances;
- Identify those MEFs that provide vital interdependent support to an MEF performed by another Federal executive department or agency or an Emergency Support Function under the National Response Plan;

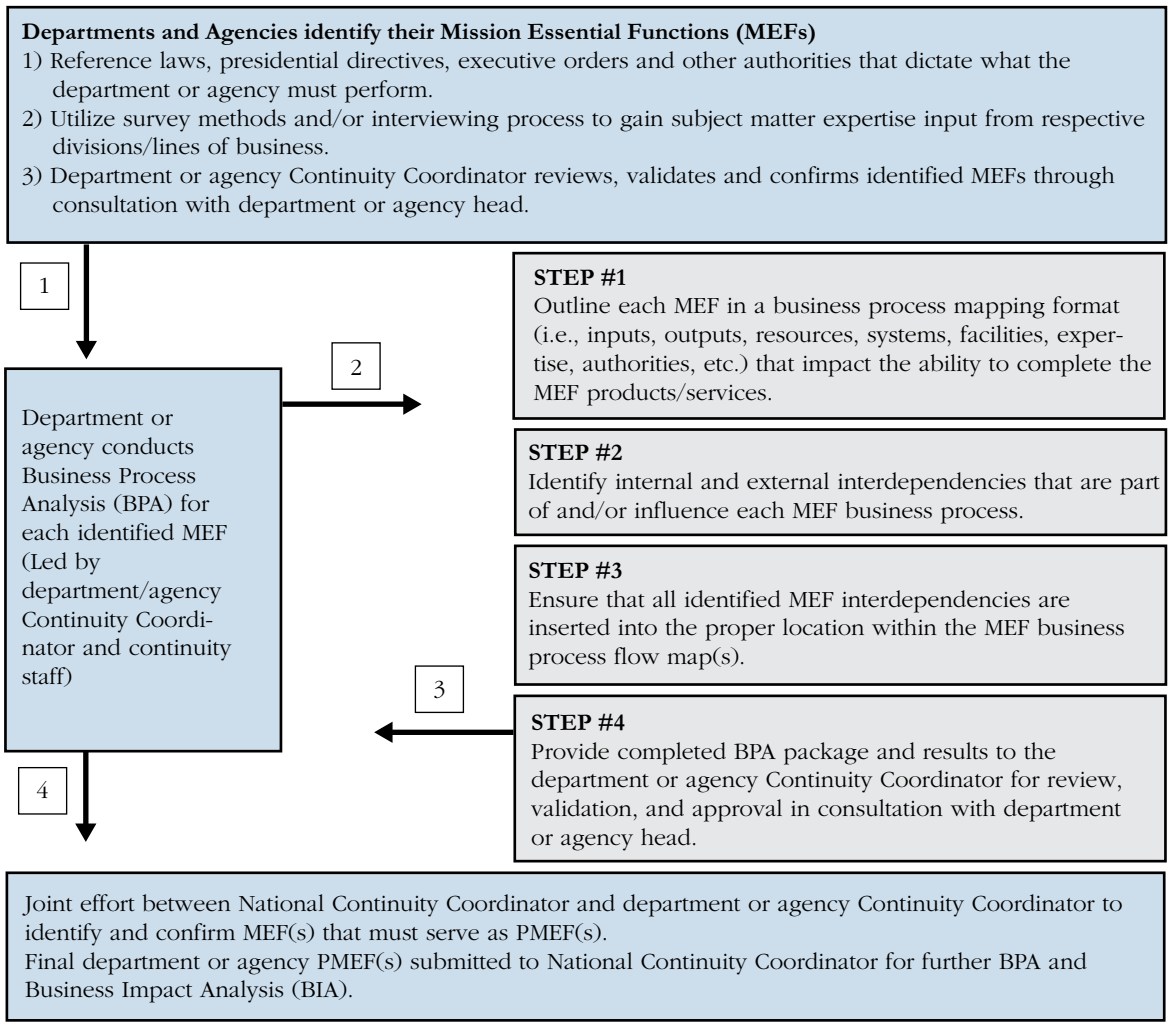
The National Response Plan defines "Emergency Support Function" as "A grouping of government and certain private-sector capabilities into an organizational structure to provide support, resources, and services."

Box 8

- Identify their MEF(s) that require vital support from another Federal executive department or agency to ensure execution of their mission and identify when and where the particular interdependency is executed within the BPA business process flow; and
- Validate and approve the identified MEF and BPA analysis by the department or agency head.

Once MEFs have been identified and analyzed as described, the planning process for identifying the PMEFs can begin.

PROCESS FOR MEF IDENTIFICATION



PRIMARY MISSION ESSENTIAL FUNCTIONS

OBJECTIVE 2C – To identify Primary Mission Essential Functions.

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
The answers to both of these must be "YES" for the function to be considered a PMEF.		

Box 9

Process – PMEF Identification and Analysis:
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 diagram on Page 21 for further details):*

- 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 their relationship to the NEFs. A risk management methodology (i.e., Business Impact Analysis (BIA) or BPA) 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 PMEF, each department and agency will revisit the prioritization of their MEF recovery timelines to ensure PMEF criticality.

- The IAB will conduct a BPA to identify and map interagency PMEF processes, workflows, activities, expertise, systems, data, and facilities inherent to the interagency execution of each NEF. The BPA should also define the PMEF 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 PMEF interdependencies within each NEF to accurately depict each department or agency's PMEF execution capability and dependencies.

- The IAB will conduct NEF-specific BIAs to: (1) identify potential single points of failure(s) that may adversely affect the execution of the interagency PMEF support to NEFs; (2) define the impact of downtime (i.e., impact of delayed PMEF recovery on NEF execution); and (3) define potential PMEF process alternatives/work-around solutions.

- NEF BPA and BIA and 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 Business Process Analyses and the NEF Business Impact Analysis. Subsequently, the described risk management approach requires an emphasis on the geographic dispersion, redundancies, 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 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 departments and agencies to ensure seamless and immediate continuation of PMEF capabilities. The department and agency planning process is described in Chapter 3.

PROCESS FOR PMEF IDENTIFICATION

Interagency Board (IAB) PMEF Business Process Analysis (BPA)
IAB conducts a BPA to identify and map interagency PMEF processes, workflows, activities, expertise, systems, data, and facilities inherent to the interagency execution of the NEF.

↓

IAB PMEF Interdependencies Analysis
IAB conducts further detailed PMEF BPA to identify and map interagency PMEF interdependencies required to execute support to the NEF.

↓

IAB NEF-specific Business Impact Analysis (BIA)
IAB conducts a detailed NEF Business Impact Analysis (BIA) to:
1) Identify interagency potential single points of failure(s) which may adversely affect the execution of the NEF;
2) Define the impact of PMEF downtime and/or failure on the execution of the NEF(s);
3) Define mandated timelines for recovery for PMEF support to each NEF and
4) Identify, create, and formalize PMEF process alternatives/work-around(s) to execute NEF(s).

↓

Interagency Board (IAB) submits NEF BPA & BIA reports to National Continuity Coordinator (NCC)
IAB compiles and submits final NEF BPA Mapping and BIA Report with findings and recommendations for mitigation, risk reduction, and risk management actions for each NEF. Risk management options shall include policy development, business process reengineering, asset dispersion, continuity system(s) design redundancy and survivability requirements, and other relevant options.

↓

NCC reviews BPA/BIA findings to:
1) Identify Continuity Program shortcomings;
2) Determine program shortcomings to initiate policy revision and development efforts;
3) Define future Continuity Program requirements and standards of performance;
4) Relate Continuity Program budget and funding requirements to risk management; and
5) Manage and lead the Federal Government Continuity Program efforts as the NCC.

OBJECTIVE 2D – To establish roles, responsibilities, and actions for the Nation's senior continuity officials.

ROLES, RESPONSIBILITIES, AND ACTIONS

President

The President leads the activities of the Federal Government for Enduring Constitutional Government.

The National Continuity Coordinator (NCC)

The Assistant to the President for Homeland Security and Counterterrorism (APHS/CT) is the NCC. The NCC is responsible for coordinating, without exercising directive authority, the development and implementation of continuity policy for executive branch departments and agencies. The NCC will periodically review and, as necessary, coordinate the revision of the National Essential Functions (NEFs). The NCC will maintain and revise as necessary the various department and agency PMEFs and MEFs in order to meet requirements for continuity, including Enduring Constitutional Government (ECG), Continuity of Government (COG), and Continuity of Operations (COOP).

The NCC is responsible for overseeing the Continuity Policy Coordination Committee (CPCC), which was established consistent with Homeland Security Presidential Directive-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.

The NCC will establish a Continuity Advisory Group (CAG) as a sub-PCC group focused on interagency implementation of continuity programs. It will be comprised of Continuity Coordinators, or their designees, from Category I, II, III, and IV (identified in NSPD-51/HSPD-20 Annex A and in Appendix B of this *Plan*) executive departments and agencies. Key State and local government representatives from the National Capital Region (NCR), and representatives from the legislative and judicial branches may be invited as appropriate. The CAG shall represent the interests of departments and agencies from Categories I-IV before the CPCC. The CAG will assist its member departments and agencies in implementing directives within its scope by performing the following functions:

- Providing the forum to address issues ultimately requiring commitment of department and agency resources;
- Facilitating the exchange of information, including lessons learned, and a sensing of the member community's views;
- Facilitating the overall coordination and decision process and the initial coordination among departments and agencies of plans and procedures for shared responsibilities;
- Identifying, prioritizing, and undertaking initiatives to explore options and make recommendations; and
- Assisting in resolving conflicts as required.

The NCC will also establish an interagency board (IAB) as a working group of the CPCC to review and recommend validation of potential PMEFs submitted by departments and agencies for submission to the NCC for final approval.

Actions for the NCC

1. On an ongoing basis, provide continuity policy coordination among all departments and agencies, monitor performance, and report to the President as appropriate.
2. As required, coordinate revision of the NEFs and department and agency PMEFs and MEFs.
3. As required, ensure that the Homeland Security Council (HSC) staff conducts meetings of the CPCC.
4. Within 30 days, establish a Continuity Advisory Group (CAG).
5. Within 30 days, establish an Interagency Board (IAB) to review PMEFs.
6. Within 30 days of IAB review, consider identified PMEFs for validation and approval.
7. Within 90 days, coordinate with FEMA in developing a continuity assessment tool for the departments and agencies to measure continuity readiness against requirements contained in NSPD-51/HSPD-20 and report the continuity assessment results to the President.
8. Within the annual budget process and on an ongoing basis, assist OMB and departments and agencies with continuity budget development and prioritization, including long-term equipment life cycle replacements and upgrades.
9. On an ongoing basis, ensure coordination of continuity acquisition functions with DHS and the General Services Administration (GSA).
10. On an ongoing basis, coordinate the integration of national continuity test, training, and exercise programs.
11. Annually submit 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.

Task Box 1

The Assistant to President for National Security Affairs (APNSA)

The APNSA coordinates with the NCC on the development and implementation of continuity policy for executive departments and agencies.

The Secretary of Homeland Security

The Secretary of Homeland Security serves as the President's lead agent for coordinating continuity *operations* and *activities* of executive departments and agencies. The Secretary of Homeland Security in his lead agency role provides continuity direction, training, and coordination of continuity exercises and provides continuity program assessments to the NCC and appropriate Federal executive departments and agencies. The Secretary's continuity responsibility is in addition to his incident management responsibility (defined in Homeland Security Presidential Directive-5 of February 28, 2003 ("Management of Domestic Incidents") which identifies the Secretary as the principal Federal official for domestic incident management.

The Secretary, in coordination with the CPCC, is responsible for disseminating in a Federal Continuity Directive (FCD) (see below) the standardized process for the identification of MEFs and the identification and submission of potential PMEFs for review by the IAB, consolidating the departments' and agencies' PMEFs, and compiling and submitting potential PMEFs to the NCC. The Secretary will conduct biennial assessments of department and agency continuity capabilities and report the results to the President through the NCC. DHS will

update its training program for department and agency continuity planners with a focus on the identification of MEFs and PMEFs.

As required by NSPD-51/HSPD-20, a Federal Continuity Directive (FCD) establishes continuity planning requirements for executive branch departments and agencies. The Secretary of Homeland Security develops and promulgates FCDs in coordination with the Continuity Policy Coordination Committee.

Box 10

The Secretary, through the National Communications System, is responsible for developing, implementing, and maintaining a comprehensive Continuity Communications Architecture (CCA), in consultation with the APHS/CT, the APNSA, the Director of the Office of Management and Budget, the Director of the Office of Science and Technology Policy (OSTP), the Chief of Staff to the President, and the Secretary of Defense. The CCA is especially important to support the National Command and Coordination Capability (NCCC) which provides the President and the Vice President with the ability to respond deliberately and appropriately to any crisis. The Secretary is also responsible for conducting quarterly and annual assessments of continuity communications capabilities in consultation with an official designated by the Chief of Staff to the President.

The Secretary is responsible for developing, leading, and conducting the Federal executive branch continuity training and exercise program, which shall be incorporated into the National Exercise Program (NEP) developed pursuant to Homeland Security Presidential Directive-8 of December 17, 2003 ("National Preparedness"), in consultation with an official designated by the Chief of Staff to the President. The NEP utilizes the Homeland Security Exercise and Evaluation Program (HSEEP) as the common exercise methodology. HSEEP is a capabilities and performance-based exercise program that provides standardized policy, doctrine, and terminology for the design, development, conduct, and evaluation of homeland security exercises. HSEEP also provides tools and resources to facilitate the management of self-sustaining homeland security exercise programs.

The Secretary shall coordinate 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.

The Secretary will develop and promulgate continuity planning guidance to non-Federal Governments and others to ensure that the National Preparedness Goal, the Target Capabilities List, and State and Local Homeland Security Grant Programs criteria provide guidance on continuity priorities and implementation guidelines. 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.

The Secretary will establish regional and State-level Continuity Working Groups (CWGs) to provide critical infrastructure assistance and support for the Nation's continuity of operations plans and programs in accordance with guidance in HSPD-7. Councils and committees established to support the National Infrastructure Protection Plan will provide members to and support the activities of the DHS/FEMA CWGs. These working groups will, at a minimum, conduct annual continuity conferences to address joint Federal and non-Federal Government continuity planning and other elements of a viable continuity program.

Actions for the Secretary of Homeland Security

1. On an ongoing basis, serve 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 perform the responsibilities set forth in NSPD-51/HSPD-20 and in HSPD-5.
2. On an ongoing basis, ensure 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 and incident management activities.
3. On an ongoing basis, ensure 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.
4. On an ongoing basis, ensure that DHS makes available continuity planning and exercise funding in the form of grants as provided by law, to State, local, territorial, and tribal governments.
5. On an ongoing basis, ensure 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 Critical Infrastructure and Key Resources (CI/KR) on continuity priorities and implementation guidelines.
6. Not less than quarterly, conduct assessments of continuity communications capabilities in consultation with an official designated by the Chief of Staff to the President.
7. Within 60 days, establish a familiarization briefing on MEF and PMEF identification for department and agency Continuity Coordinators (Assistant Secretary-level).
8. Within 60 days, in coordination with the Continuity PCC, issue a Federal Continuity Directive on Continuity Requirements, to include the formalized process for departments and agencies to identify MEFs, and revise through annual, or as needed, Directives thereafter.
9. Within 60 days, in coordination with the Continuity PCC, issue a Federal Continuity Directive on the formalized process for department and agency submission of potential PMEFs that are consistent and supportive of the NEFs.
   - Include a standardized checklist to allow departments and agencies to assess their PMEFs through a risk management process;
   - Include guidance on how the PMEF link to/supports NEF(s); and
   - Include guidance on impact statements if a specific PMEF is not conducted.
10. Within 30 days after submission of department and agency MEFs and potential PMEFs, compile submissions and provide them to the NCC for IAB review and validation.
11. Within one year and annually thereafter, update training courses for department and agency continuity planners on the identification and development of PMEFs and MEFs, in addition to maintaining ongoing continuity training courses.
12. 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), provide the Director of OSTP and DOD with an implementation plan for a comprehensive Continuity Commu-

nications Architecture (CCA), which shall include the minimum requirements necessary to finalize selection of a secure communications system by DOD.

11. Within 90 days after receipt of technical requirements from OSTP, through the NCS, develop, implement, and begin maintenance of a comprehensive CCA.
14. On an annual basis, develop, lead, and conduct an integrated (COOP and COG) continuity training exercise, incorporated into the National Exercise Program, and report the results to the NCC.
15. On an as needed basis, revise and promulgate integrated continuity planning guidance to non-Federal Governments and others as appropriate.
16. On an as needed basis, provide critical infrastructure assistance and support in accordance with HSPD-7 and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*.
17. On an as needed basis, provide cybersecurity assistance and support in accordance with HSPD-7 and the *National Strategy to Secure Cyberspace*.
18. Develop regional and state level Continuity Working Groups to, at a minimum, conduct annual continuity conferences to address joint Federal and non-Federal Government continuity planning and other elements of a viable continuity program.

Task Box 2

Continuity Coordinators

The *Policy* requires department and agency heads to appoint a senior accountable official, at the assistant secretary or equivalent level, to be the organization's Continuity Coordinator responsible for working with the organization head to ensure the organization's continuity capability. For those departments and agencies on the Continuity PCC, the Continuity Coordinator represents their organization and offers practical recommendations on continuity policy. Continuity Coordinators, or their designee, represent their department or agency on the CAG. Continuity Coordinators will also work with their department or agency heads to complete the MEF and PMEF identification process articulated in this chapter.

Continuity Managers

Under the direction of each department or agency head, Continuity Managers manage day-to-day continuity programs and represent their department or agency on the CAG and working groups as appropriate. The continuity program of each department or agency, led by Continuity Managers, report to the Continuity Coordinator.

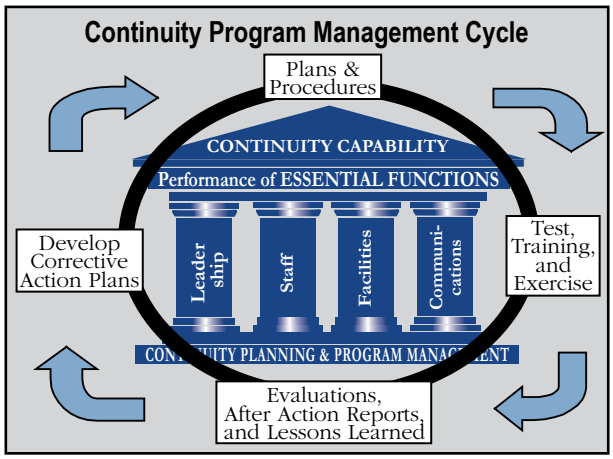
GOAL #3 To ensure continuity readiness procedures and metrics.

INTRODUCTION

Development of an effective continuity program begins with a review and identification of all of an organization's responsibilities and functions as they relate to the four key continuity pillars. Once Essential Functions are prioritized and resourced, a process must be used to ensure that the functions can be sustained under an all-hazards threat environment.

OBJECTIVE 3A – To establish a Continuity Program Management Cycle.

A standardized Continuity Program Management Cycle ensures consistency across all government continuity plans and establishes consistent performance metrics, prioritizes implementation plans, promulgates best practices, and facilitates consistent cross-agency continuity evaluations. A cyclical model of planning, training, evaluating, and implementing corrective actions provides key leaders and essential personnel the baseline information, awareness, and experience necessary to fulfill their continuity program management responsibilities. Objective evaluations and assessments, developed from tests and exercises, provide feedback on continuity planning, procedures, and training. This feedback supports a corrective action process, which helps to establish priorities, informs budget decision-making, and drives improvements in plans and procedures. The Continuity Program Management Cycle, as indicated below, is the process all organizations should use in developing and implementing their continuity program.



Box 11

OBJECTIVE 3B – To establish continuity requirements and metrics.

KEY CONSIDERATIONS

Plans and Procedures

Departments and agencies shall develop and maintain continuity plans and procedures that, when implemented, provide for continued performance of their MEFs, as required, continued performance of their PMEFs under all circumstances, and integration with other governmental and non-governmental organizations as appropriate. Each individual department or agency program should be tailored to its respective organization, separate but consistent with and complementary to DHS's Test, Training, and Exercise Program. The continuity plan must do the following:

a. Identify MEFs and PMEFs as described in Chapter 2.

b. Establish orders of succession and pre-planned delegation and devolution of authorities that ensure an orderly, and pre-defined, transition of leadership and

delegation of authority within a department or agency through any emergency for the agency head and supporting key positions. Succession orders and delegations of authority must be planned and documented in advance in accordance with applicable laws to ensure the performance of the department or agencies MEFs and PMEFs.

c. Identify and establish procedures to ensure vital resources, facilities, and records are safe-guarded, available, and accessible to support continuity operations. Vital resources should include personnel, equipment, systems, infrastructures, supplies, and other assets required to perform the department or agency's MEFs and PMEFs.

d. Identify provisions for the acquisition of necessary resources for continuity of operations on an emergency basis.

e. Identify and provide for the availability and redundancy of critical communications capabilities at primary sites, alternate sites, and in transit in order to ensure the performance of department and agency MEFs and PMEFs, and support connectivity between and among key government leadership, internal elements, other executive departments and agencies, critical partners, and the public. Category I and select Category II departments and agencies shall coordinate with the Secretary of Homeland Security and the Secretary of Defense to obtain and operate secure, integrated, Continuity of Government communications.

f. Provide for the ability to recover or reconstitute from the effects of an emergency and return to a fully operational condition. Departments and agencies shall conduct the coordination and planning necessary to return to normal operations.

g. Identify the components, processes, and requirements for the identification, training, and preparedness of personnel capable of relocating to alternate facilities to support the continuation of the performance of MEFs and PMEFs.

h. Identify the components, processes, and requirements that ensure the continued performance of the department or agency's MEFs and PMEFs.

i. Establish alert and notification procedures to include the process for monitoring the DHS Homeland Security Advisory System, intelligence, and other advisory information. Establish internal procedures for executing changes to the COGCON or other Regional, State, territorial, tribal or private continuity preparedness or activation direction. Provide for the process of reporting continuity readiness and activation status.

Budgeting for continuity capabilities is one of the most important components of continuity planning. Departments and agencies need to formulate and prioritize budget requests after application of the continuity requirements listed in NSPD-51/HSPD-20 *(see below)*. Appendix F also includes metrics to be used to measure ability to meet the continuity requirements.

Continuity requirements for the Executive Office of the President (EOP) and executive branch departments and agencies shall include the following (NSPD-51/HSPD-20 Paragraph 11):

- 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;

- 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;

- Vital resources, facilities, and records must be safeguarded, and official access to them must be provided;
- Provision must be made for the acquisition of the resources necessary for continuity operations on an emergency basis;
- 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;
- Provision must be made for reconstitution capabilities that allow for recovery from a catastrophic emergency and resumption of normal operations; and
- 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

Box 12

Test, Training, and Exercise (TT&E)

An effective TT&E program is necessary to assist departments and agencies to prepare and validate their organization's 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 department and 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 a subsequent improvement. All agencies must plan, conduct, and document periodic tests, training, and exercises 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 Corrective Action Program (CAP) (described below).

DHS, in coordination with the CPCC, shall develop Federal Continuity Directives that identify specific TT&E requirements, including required continuity training, types and frequency of exercises, and assessment criteria to ensure departments and agencies develop and maintain a robust TT&E program. TT&E programs will seek to accomplish the following goals:

- Communicate objectives, expectations, and the definition of success for all phases of continuity operations;
- Improve accountability for coordinating and de-conflicting continuity requirements across executive departments and agencies, across levels of government, and with the private sector;
- Establish a framework of performance criteria to measure and evaluate progress and achievement of continuity requirements within each department and agency and across departments and agencies;
- Include annual continuity training and assessment requirements and development of procedures for identifying best practices and corrective action;

- Test the viability of communications systems;
- Include continuity exercises, which are incorporated into the National Exercise Program;
- Include development of continuity alert and notification procedures and tests, and integrate these into continuity training and exercise activities; and
- Provide input into development of corrective action plans.

DHS, in coordination with State, territorial, tribal, and local jurisdictions, and private sector critical infrastructure owners and operators, shall also develop continuity guidance to assist these jurisdictions with development of their TT&E programs.

Evaluations and Assessments

Evaluations and assessments provide critical feedback on how well TT&E programs are preparing leadership, staff, and organizations to meet their continuity requirements. At a minimum, all organizations should conduct and document annual assessments of their continuity TT&E programs and continuity plans and programs. DHS will disseminate FCDs with detailed procedures for evaluations and assessments. Additionally, DHS, in coordination with the other Federal executive departments and agencies, will conduct an annual, integrated, interagency continuity exercise to test the executive branch's ability to conduct its continuity programs, and shall prepare a consolidated assessment report on the continuity status of the executive branch for the NCC.

Additionally, departments and agencies will provide continuous readiness status information through FEMA's Readiness Reporting System (RRS).

The Readiness Reporting System (RRS) provides the status of the Federal executive branch departments and agencies to perform their PMEFs in support of the NEFs. The RRS is used to conduct assessments and track capabilities at all times under all conditions, including natural disasters, man-made incidents, terrorism, and war.

Box 13

Corrective Action Program (CAP)

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 CAP is to accomplish the following:

- Identify continuity deficiencies and other areas requiring improvement and provide responsibilities and a timeline for corrective action;
- Identify program and other continuity funding requirements for submission to department and agency leadership and OMB;
- Identify and incorporate efficient acquisition processes, and where appropriate, collect all interagency requirements into one action; and
- Identify continuity personnel requirements for department and agency leadership and their supporting Human Resource Offices and the Office of Personnel Management (OPM).

DHS will integrate areas requiring corrective action that affect multiple departments and agencies into the CAP established by HSPD-8. Specific guidance and requirements for the department and agency CAP shall be addressed in Federal Continuity Directives.

OBJECTIVE 3C – To establish roles, responsibilities, and actions for continuity officials.

ROLES, RESPONSIBILITIES, AND ACTIONS

Heads of Federal Executive Departments and Agencies

Heads of Federal executive departments and agencies are responsible for **integrating continuity planning as a fundamental part of everything that they do**. One of the primary goals of continuity planning is to ensure that departments and agencies are able to perform their Primary Mission Essential Functions—which support the **continuing performance of National Essential Functions—under all conditions, with and without warning**. Department and agency heads will appoint a senior accountable official, at the Assistant Secretary or equivalent level, as the Continuity Coordinator for the department or agency. Departments and agencies will emphasize geographic dispersion of leadership, staff, and infrastructure, as appropriate, in order to increase survivability and maintain uninterrupted Government Functions. Departments and agencies will be able to execute continuity plans and will comply with the requirements and assigned responsibilities under the COG-CON program.

Department and agency heads will identify and submit to the NCC through the IAB their respective MEFs and potential PMEFs that support NEFs. In consultation with the NCC, heads of departments and agencies are responsible for the periodic review and revision of their PMEFs and MEFs. During development of PMEFs, departments and agencies will coordinate and integrate 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. The heads of department and agencies must ensure that their key leaders and support staff are provided annual familiarization training on PMEFs and MEFs.
Heads of departments and agencies are responsible for participating in the Federal executive branch continuity test, training, exercise, and assessment programs, which shall be incorporated into the National Exercise Program developed pursuant to HSPD-8. Testing should ensure viability of communications systems.

For continuity funding requests, department and agency heads will incorporate Office of Management and Budget (OMB) guidance from Circular A-11 guidance to ensure proper accounting of homeland security related spending. Department and agency heads will also submit required performance data through FEMA's Readiness Reporting System (RRS) and required continuity reports. These assessments will be used to determine an organization's continuity capability and to help identify needs and gaps.

Actions for the Heads of Federal Executive Departments and Agencies

1. On an ongoing basis, ensure performance of department or agency Primary Mission Essential Functions.
2. On an ongoing basis, incorporate continuity requirements into daily department and agency operations.
3. On an ongoing basis, ensure the department or 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 and other essential functions.
4. Within 30 days, appoint a senior accountable official, at the Assistant Secretary or equivalent level, as the Continuity Coordinator for the department or agency.

5. Within 30 days and annually thereafter, submit a report to the NCC certifying that the department or agency has a continuity capability plan that includes the items in Paragraph 11 of NSPD-51/HSPD-20 (see Box 12).
6. On an ongoing basis, consistent with sections 11(e) and 19(c) of NSPD-51/HSPD-20, plan, program, and budget for secure continuity communications capabilities.
7. Within 90 days after DHS' guidance, review and revise MEFs and identify and submit potential PMEFs.
8. Within 30 days after validation of department and agency PMEFs and annually thereafter, ensure key leaders and support staff are provided familiarization training of department or agency PMEFs and MEFs.
9. Within 180 days after validation of department and agency PMEFs, ensure PMEF and MEF interdependencies are coordinated internally, at the interagency level, and with private sector partners.
10. On an ongoing basis, participate in DHS's National Exercise Program.
11. On an ongoing basis, incorporate OMB Circular A-11 guidance, or other OMB guidance on continuity as provided, when developing continuity budgets.
12. As required, submit Continuity Readiness Reports, and other reports as requested, through the Readiness Reporting System.

Task Box 3

The Director of the Office of Management and Budget

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 NCC, issues guidance to assist departments and agencies with continuity budget submissions.

Actions 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 executive department and agency continuity funding requests and performance data that are submitted by executive branch departments and agencies as part of the annual budget request process in order to monitor progress in the execution of this *Plan* and continuity budgets.
3. Annually reconcile department and agency continuity funding requests and performance data with Continuity Readiness Reporting and annual continuity assessments compiled by FEMA.

Task Box 4

The Director of the Office of Science and Technology Policy

The Director of the Office of Science and Technology Policy (OSTP) defines and issues minimum requirements for continuity communications for executive departments and agencies in consultation with the APHS/CT, the APNSA, the Director of OMB, and the Chief of Staff to the President. The Director establishes requirements for, and monitors the development, implementation, and maintenance of a comprehensive Continuity Communications Architecture to integrate continuity components in consultation with the APHS/CT, the APNSA, the Director of OMB, and the Chief of Staff to the President. In performing those tasks, the Director of OSTP will also consult with the Secretaries of Defense and Homeland Security because of their significant roles in implementing the minimum continuity communications requirements and the Continuity Communications Architecture. In order to support those tasks and to aid in ensuring the success of the Continuity Communications Architecture, the Director of OSTP will establish and chair a Continuity Communications Architecture Board (CCAB). The Director of OSTP also reviews quarterly and annual assessments of continuity communications capabilities and reports the results and recommended remedial actions to the NCC.

Actions for the Director of the Office of Science and Technology Policy

1. Annually review and revise 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. Within 60 days, establish and chair a Continuity Communications Architecture Board (CCAB).
3. Within 30 days after validation of PMEFs, distribute requirements for, and update as needed, a comprehensive Continuity Communications Architecture (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, monitor 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, review assessments of continuity communications capabilities and report the results and recommended remedial actions to the NCC.

Task Box 5

An official designated by the Chief of Staff to the President

Recognizing that each branch of the Federal Government is responsible for its own continuity programs, an official designated by the Chief of Staff to the President shall ensure 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 assets efficiently to maintain a functioning Federal Government. This individual will advise the President, the Chief of Staff to the President, the APHS/CT, and the APNSA on COGCON operational execution options; and consult with the Secretary of Homeland Security in order to ensure synchronization and integration of continuity activities among the four categories of executive departments and agencies.

Actions for an official designated by the Chief of Staff to the President

1. On an ongoing basis, advise the President, Chief of Staff to the President, the APHS/CT, and the APNSA on COGCON operational execution options.
2. On an ongoing basis, ensure 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, consult with the Secretary of Homeland Security in order to ensure synchronization and integration of continuity activities among the four categories of executive departments and agencies.

Task Box 6

Secretary of Defense

The Department of Defense (DOD) performs a significant role in assisting other Federal executive departments and agencies with communications systems and other support assets. The Secretary of Defense, in coordination with the Secretary of Homeland Security as Executive Agent of the National Communications System, is responsible for providing secure, integrated, Continuity of Government communications to the President, the Vice President, and, at a minimum, Category I executive departments and agencies. These communications shall be an integral component of the Continuity Communications Architecture. DOD will assist DHS in conducting continuity training and exercises and in providing continuity of operations assistance during emergencies and disasters.

Actions for the Secretary of Defense

1. Within 60 days after the publication by DHS of the Continuity Communications Architecture implementation plan, identify the secure, integrated, Continuity of Government communications for use by the President, the Vice President, and, at a minimum, Category I executive departments and agencies.
2. Upon identification and implementation, continuously maintain the secure, integrated, Continuity of Government communications for the President, the Vice President, and, at a minimum, Category I executive departments and agencies.
3. Not less than quarterly, assist 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, assist DHS in conducting continuity training and exercises and in providing assistance during emergencies and disasters.

Task Box 7

Director of National Intelligence

The Director of National Intelligence, in coordination with the Attorney General and the Secretary of Homeland Security, shall produce and submit to the President a biennial assessment of the foreign and domestic threats to the Nation's Continuity of Government.

Actions for the Director of National Intelligence

1. Every two years, produce an assessment for the NCC of the foreign and domestic threats to the Nation's Continuity of Government.
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, provide geospatial continuity operational support to DHS to assist in response and recovery operations.

Task Box 8

The Secretary of Homeland Security

The Administrator of the Federal Emergency Management Agency (FEMA) is responsible for coordinating the implementation, execution, and assessment of continuity activities and programs. Upon establishment of the Continuity Advisory Group (CAG), FEMA's Continuity Coordinator will chair regular meetings and report to the CPCC on the activities of the CAG.

In coordination with the CAG and in consultation with the CPCC, DHS/FEMA will develop and promulgate Federal Continuity Directives that establish continuity planning requirements, including continuity plan templates to assist departments and agencies and others in developing internal continuity processes and procedures, TT&E programs, and assessment criteria for executive departments and agencies.

In accordance with Federal Continuity Directives, FEMA will conduct biennial assessments of individual department and agency continuity capabilities and report the results to the NCC through the Secretary of Homeland Security.

FEMA will develop, operate, and maintain a continuity Readiness Reporting System (RRS) which will measure and report both the individual and aggregate ability of departments and 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.

Actions for the Secretary of Homeland Security

1. Within 90 days, coordinate with the APHS/CT in developing a continuity assessment tool for the departments and agencies to measure continuity readiness against requirements contained in NSPD-51/HSPD-20.
2. Quarterly, ensure FEMA's Continuity Coordinator chairs meetings of the CAG and reports to the Continuity PCC.
3. Every two years, conduct department and agency assessments of continuity capabilities and report the results to the NCC.
4. On an ongoing basis, operate and maintain the Readiness Reporting System.
5. On an as needed basis in coordination with the CAG and in consultation with the CPCC, develop and promulgate Federal Continuity Directives that establish continuity planning requirements, continuity plan templates, TT&E programs, and assessment criteria.
6. On an ongoing basis, ensure that the FEMA Operations Center (FOC) maintains 24-hour operations to ensure appropriate procedures for emergency operations. *(See further discussion of the FOC in Chapter 2.)*

Task Box 9

Director of the Office of Personnel Management (OPM)

The Director of OPM will provide guidance to departments and agencies on developing personnel policies that address continuity plans and procedures, including alternate work options. The Director, in coordination with the Secretary of Homeland Security, will provide guidance to and coordinate with the Federal Executive Boards (FEBs) to assist in facilitating planning meetings and exercises to develop effective continuity programs among participating Federal executive departments and

agencies and, where appropriate, non-Federal Government entities, including respective State, local, territorial, and tribal governments and private sector owners and operators of critical infrastructure in their planning and preparedness activities.

The Director of OPM will consider creation of an occupational specialty for continuity and an associated training program to acknowledge the emerging, critical importance of continuity knowledge, skills, and abilities to achieve a continuity capability in today's environment.

Actions for the Director of the Office of Personnel Management

1. Within 120 days, develop and promulgate personnel guidance to support Federal executive branch continuity plans and programs.
2. Within 120 days, establish telework guidance to support department and agency continuity programs.
3. Within 120 days, in coordination with the Secretary of Homeland Security, provide guidance and coordinate with the Federal Executive Boards (FEB) to assist in facilitating planning meetings and exercises to develop effective continuity programs.
4. On an ongoing basis, assist DHS in conducting continuity training, exercises, assessments, and other preparedness activities.
5. Within 120 days, submit a report to the NCC on the possibility of creating an occupational specialty for continuity and an associated training program, and, if approved, work with FEMA to include the information in a Federal Continuity Directive.

Task Box 10

Administrator of the General Services Administration (GSA)

The Administrator of GSA will coordinate the provision of executive branch facilities to support continuity operations and maintain the database for all department and agency alternate facilities. In order to help facilitate a coordinated and seamless executive branch continuity infrastructure, GSA shall provide and maintain a centralized procurement function for all department and agency continuity infrastructure requirements. GSA shall also assist DHS in conducting continuity training and other preparedness activities and assist DHS and the departments and agencies in their recovery and reconstitution during and in the aftermath of emergencies and disasters.

Actions for the Administrator of the General Services Administration

1. On an ongoing basis, coordinate the provision of executive branch facilities to support continuity operations and maintain the database for all department and agency alternate facilities.
2. On an ongoing basis, facilitate a coordinated and seamless executive branch continuity infrastructure and provide and maintain a centralized procurement system for all department and agency continuity infrastructure requirements.
3. On an ongoing basis, assist the Secretary of Homeland Security in conducting continuity tests, training, exercises, assessments, and other preparedness activities.
4. During and in the aftermath of emergencies and disasters, assist the Secretary of Homeland Security and affected departments and agencies in their recovery and reconstitution.

Task Box 11

Small Agency Council

The Small Agency Council (SAC), in coordination with DHS, will provide a forum for development and integration of continuity policies and programs among the Federal Government organizations represented on the council.

Actions for the Chairman of the Small Agency Council

1. On an ongoing basis, in coordination with the Secretary of Homeland Security, provide a forum for development and integration of continuity policies and programs among the Federal Government organizations represented on the Council.

Task Box 12

Federal Executive Associations (FEAs)

FEAs shall provide assistance where practicable in coordinating continuity activities for FEA members.

Actions for the Federal Exective Associations

1. On an ongoing basis, provide assistance where practicable in coordinating continuity activities for FEA members.

Task Box 13

Coordination, Communication, and Integration

Chapter 4

GOAL #4 **To promote interoperability.**

INTRODUCTION

This *Implementation Plan* provides direction to Federal executive branch departments and agencies. However, the continuation of our constitutional form of government, the continuation of our National Essential Functions, and the resumption or continuation of functions to support the public are also critically dependent on the effective functioning of all three branches (legislative, executive, and judicial) of the Federal Government; the State, local, territorial and tribal government structures; and key private sector entities.

This chapter explains how the continuity concepts discussed throughout the *Implementation Plan* are relevant to those key partners and suggests implementation measures that should be taken to ensure that essential services are continued; law and order is maintained; and the principles of our Constitution are preserved. The concepts of sustained leadership, available key emergency personnel, interoperable communications, viable operating locations, and a focus on continuing essential functions involves all levels of the government and key private sector entities.

The chapter contains three sections addressing coordination, communication, and integration:

- Chapter 4A: Among the three branches of the Federal Government;
- Chapter 4B: Among Federal, State, local, territorial, and tribal governments; and
- Chapter 4C: Between private sector critical infrastructure owners and operators and all levels of the government.

OBJECTIVE 4A – To promote interoperability among the branches of the Federal Government.

INTRODUCTION

A cooperative effort among the legislative, executive, and judicial branches of the Federal Government, referred to as Enduring Constitutional Government (ECG), is essential to preserving the powers granted to the people of the United States by the Constitution. It is imperative that all three branches of the Federal Government are able to execute their constitutional responsibilities, maintain interoperability, and support the eight National Essential Functions (NEFs) (as discussed in Chapter 2). This is especially true during catastrophic emergencies in order to preserve our Nation's constitutional government and maintain the functions of the Federal Government.

The Legislative Branch consists of the Senate, the House of Representatives, and their respective supporting organizations. The Judicial Branch consists of the Supreme Court of the United States, courts established under Article III by the Congress, and their supporting organizations.

KEY CONSIDERATIONS

Each of the three branches of government has unique but mutually supporting powers to ensure the continuance of its respective constitutional role. By performing those constitutional roles, the legislative, executive, and judicial branches, individually and collectively, support the ability of the Federal Government to perform NEFs, continue ECG, and ensure that essential services are provided to the Nation's citizens. 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. Sustaining the 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.

ROLES AND RESPONSIBILITIES

Recognizing that each branch of the Federal Government is responsible for its own continuity programs, the appropriate senior decision-makers of all three branches are encouraged to coordinate their continuity plans where appropriate. The executive branch shall provide the support described in NSPD-51/HSPD-20 to the legislative and judicial branches to ensure interoperability, inclusion in appropriate continuity plans, and allocation of national assets to maintain a functioning Federal Government.

While this *Plan* serves as an implementation of the executive branch's continuity policy, and in order to support constitutional roles and responsibilities, the appropriate senior decision-makers of the legislative and judicial branches are encouraged to also review their prioritized goals and objectives, concept of operations, and procedures for continuity and incident management activities on a regular basis in order to accomplish the following:

- Maintain branch essential functions and supporting activities;
  - Legislative examples could include representing constituents, passing bills, coordinating between the two chambers of Congress, communicating with the executive and judicial branches, etc.; and
  - Judicial examples could include communicating with the legislative and executive branches, hearing arguments, issuing opinions, etc.

- Perform branch essential functions and support activities during any emergency;
- Provide for capabilities that allow for recovery from a catastrophic emergency and resumption of normal operations;
- Provide for the acquisition of resources necessary for continuity operations on an emergency basis;
- Safeguard vital resources, facilities, and records, and provide official access to them;
- Maintain and integrate effective, redundant, survivable continuity communications systems at daily operating sites and alternate facilities in order to support connectivity between and among key Federal Government leadership and the public;
- Provide for the identification, training, and preparedness of personnel capable of relocating to alternate facilities where necessary to support the continuation of the performance of branch essential and support functions; and
- Facilitate effective implementation of the provisions of the Constitution concerning succession to the Presidency or the exercise of its powers, and the Presidential Succession Act of 1947 (3 U.S.C. § 19). The executive branch will ensure that appropriate support is available to the Vice President, the Speaker of the House, and the President Pro Tempore of the Senate. The Vice President, the Speaker of the House, and the President Pro Tempore should be prepared at all times to execute their role as a successor President.

ACTIONS AND EXPECTATIONS

The legislative, executive, and judicial branches will continue cooperation to ensure interoperability, integration, and appropriate allocation of national assets to ensure Federal Government continuity. Supporting organizations will develop and execute appropriate memoranda of understandings and agreements to formalize continuity plans and procedures.

The appropriate senior decision-makers of the legislative and judicial branches, through established channels with the executive branch, should continue to:

- Coordinate the implementation and execution of continuity operations and activities with the executive branch;
- Maintain comprehensive continuity communications; and
- Conduct continuity tests, training, and exercise programs independently and in coordination with the executive branch.

OBJECTIVE 4B – To promote interoperability among Federal, State, local, territorial, and tribal governments.

INTRODUCTION

By continuing the performance of essential functions through a catastrophic emergency, the State, local, territorial, and tribal governments (non-Federal Governments entities or NFGs) support the ability of the Federal Government to perform NEFs, continue Enduring Constitutional Government, and ensure that essential services are provided to the Nation's citizens. A comprehensive and integrated continuity capability will enhance the credibility of our national security posture and enable a more rapid and effective response to, and recovery from, a national emergency.

KEY CONSIDERATIONS

To create a seamless continuity structure, NFGs should develop essential functions analogous to the PMEFs described in Chapter 2. Identification of activities that support the essential functions enables an NFG to plan for and develop effective continuity measures and programs. Redundant, interoperable communications systems will facilitate survivability and permit effective coordination during an emergency. The concept of interoperability includes not only compatible systems and frequencies among all continuity stakeholders but also lists of key contacts for NFGs and Federal counterparts.

Development of NFG continuity programs is essential to effective Federal continuity efforts. Rapid and effective response to, and recovery from, the domestic consequences of an attack or other incident requires continued performance of NFG missions. By assuring the health, safety, and welfare needs of citizens and clients, NFGs perform a critical role in support of essential functions and services. By maintaining financial stability, NFGs support the protection and stabilization of the Nation's economy and ensure public confidence in its financial systems. By bringing to justice perpetrators of crimes or attacks against the United States or its people, property, and infrastructure, NFGs maintain law and order and sustain public confidence in its governmental institutions.

To help ensure that NFGs are prepared to support their essential functions, each should consider creating a "continuity readiness posture" similar to the Federal Executive Branch's Continuity of Government Readiness Conditions (COGCON) system as discussed in Chapter 2.

ROLES AND RESPONSIBILITIES

The responsibility for preparing and responding to emergencies is shared by the Federal Government, State, local, territorial, and tribal governments and the private sector. All have important and interdependent roles in preparing for, responding to, and recovering from natural or manmade incidents or disasters.

The Executive Branch of the Federal Government

Close cooperation is essential among the large and varied community of NFGs and with the Federal Government for coordinated, effective continuity programs. Federal executive departments and agencies should coordinate with NFGs to ensure emergency plans and capabilities are compatible, prevent redundancies, and minimize conflicting lines of authority. Existing organizations with inter-government coordination missions, such as Federal Executive Boards, shall support continuity efforts.

DHS coordinates overall domestic incident management and response procedures and is the Federal executive branch's contact for coordination with NFGs for continuity programs. DHS shall provide guidance for the integration of national continuity plans and operations with State, local, territorial, and tribal governments in order to provide for the delivery of essential services during an emergency. The National Infrastructure Protection Plan and the supporting organizations established under HSPD-7 provide support to the Nation's continuity plans and programs. To promote rapid continuity program implementation and further integration of continuity efforts across government entities and the private sector, DHS will make available continuity planning and exercise funding in the form of grants as provided by law to NFGs.

The Federal intelligence and law enforcement agencies will share relevant and useful intelligence and law enforcement information with NFGs, as appropriate, using existing processes and communications methods.

State, Local, Territorial, and Tribal Governments

NFGs are encouraged to develop a robust continuity program to ensure that essential functions are performed. The initial step is to identify the essential functions and the supporting activities that are critical to continue during an emergency. Further discussion on this process is found in Chapter 2. NFGs are encouraged to establish continuity programs that facilitate the performance of essential functions during any emergency for a period of up to 30 days or longer, 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.

Each NFG should identify successors, put in place emergency delegations of authority, and plan for geographic dispersion of staff and infrastructure where appropriate. Safeguarding of vital resources, facilities, and records will facilitate continuity efforts. A plan to provide for the acquisition of resources serves both the NFG and the larger national continuity program. These actions will permit timely reconstitution and recovery from catastrophic emergencies and resumption of normal operations. NFGs are encouraged to share intelligence and law enforcement information through established channels with the Federal Government where relevant and useful, especially through the Homeland Security Information Network (HSIN) and the Homeland Secure Data Network (HSDN).

Availability, redundancy, and connectivity of communications between and among NFGs, key Federal Government leadership, and the public is a critical capability necessary for sustained operations through a crisis. Tools that can be used to help on this front include the Emergency Alert System (EAS), the Integrated Public Alert Warning System (IPAWS), the National Alert Warning System (NAWAS), and the Washington Metropolitan Area Warning System (WAWAS).

The large and diverse universe of State, local, territorial, and tribal governments makes it imperative that each consider the others' essential function requirements and responsibilities, communication capabilities, and needs. It is also essential that NFGs utilize their existing relationships with DHS and consistently update all essential contact information.

Development of a strong continuity program is only the first step. Identification and training of personnel capable of relocating to alternate or other continuity facilities where necessary to support the continuation of the performance of PMEFs and essential functions is also required. The National Preparedness System, established by HSPD-8, provides guidance for the Federal executive branch and NFGs in coordinating capabilities to prevent, protect against, respond to, and recover from all-hazards in a way that balances risk with resources and includes exercises, assessments, and reporting requirements. The Federal Government and all citizens rely

immensely on officials at the local level, and this will especially be true during a local emergency situation. Local emergency response and incident command personnel will be first on the scene of a crisis, and they will have the local knowledge and relationships required to successfully resolve the crisis. When a local crisis affects the performance of a critical Primary Mission Essential Function (PMEF)—and therefore a NEF—the role of local government officials and personnel cannot be understated.

ACTIONS AND EXPECTATIONS

Department of Homeland Security

- Develop and promulgate 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;

- Provide planning guidance to NFGs on development of internal Mission Essential Functions (MEFs). Guidance will be based on the requirement of continuing the performance of essential functions. (Guidance for the Federal executive branch is contained in Chapter 2 of this *Implementation Plan*);

- Make available continuity planning and exercise funding, in the form of grants as provided by law, to State, local, territorial, and tribal governments;

- Establish DHS/FEMA regional and State-level Continuity Working Groups (CWGs). These working groups will, at a minimum, conduct annual continuity conferences to address joint Federal and NFG continuity planning and other elements of a viable continuity program; and

- Provide critical infrastructure assistance and support for the Nation's continuity of operations plans and programs in accordance with guidance in HSPD-7. Organizations established to support the National Infrastructure Protection Plan will be members of and support the activities of the Continuity Working Groups.

Office of Personnel Management (OPM)

- Assure that Federal Executive Boards assist and coordinate continuity efforts before, during, and after an emergency.

Federal Intelligence and Law Enforcement Communities

- Continue providing intelligence through existing channels to NFGs as appropriate, using official processes and communications methods.

State, Local, Territorial, and Tribal Governments

The Federal Government is dependent on State, local, and other governments, especially during a crisis. Local governments provide the local law enforcement, first responders, and the first line of defense against local threats that could have national implications. As identified by the National Response Plan, the primary responsibility for initial incident response remains at the local level.

NFGs are encouraged to consider the following recommendations:

- Appoint a senior accountable official to be responsible for planning and implementation of continuity programs for the organization;

- Establish a continuity plan and program that facilitates the performance of MEFs during an emergency for a period up to 30 days or longer, until normal operations can

be resumed, and the capability to be fully operational at alternate sites or other continuity locations as soon as possible after the occurrence of an emergency, but not later than 12 hours after COOP activation;

- Develop succession orders and pre-planned devolution of authorities in accordance with applicable law;

- Develop a vital resources, facilities, and records program that ensures these are safeguarded and that there is official access to them. Develop and implement training to support this program;

- Make provisions for the acquisition of the resources necessary for continuity operations on an emergency basis;

- Provide 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, and other organizations, critical partners, and the public;

- Provide information to Federal intelligence and law enforcement agencies as appropriate and using official processes and communications methods;

- Plan, program, and budget for continuity capabilities consistent with this *Implementation Plan*, and provide to DHS grant funding requests, as provided by law;

- Plan, conduct, and support annual continuity tests, training, exercises, and assessments in order to prepare and evaluate program readiness and ensure adequacy and viability of continuity plans and communications systems;

- Participate in DHS/FEMA Regional and State Continuity Working Groups and in the annual continuity conferences conducted by DHS;

- Establish an organizational continuity working group. States may consider designating their State Emergency Management Offices to lead their respective continuity programs and working groups, with support from the National Guard, law enforcement, medical, fire, human services, and other organizations; and

- Develop interoperable communications capability with Federal, State, local, tribal, and territorial governments and other organizations as appropriate to support continuity and emergency response requirements.

OBJECTIVE 4C – To promote interoperability between the private sector critical infrastructure owners and operators and the government.

INTRODUCTION

Private Sector Critical Infrastructure Owners and Operators have a unique and invaluable role in ensuring the performance of essential functions during a catastrophic emergency. Similar to NFGs, the continued functioning of the private sector supports the ability of all levels of government to perform essential functions, continue Enduring Constitutional Government, and ensure that essential services are provided to the Nation's citizens. Private sector operation during emergencies is critical to a rapid and effective response to and recovery from a catastrophic emergency.

KEY CONSIDERATIONS

Private sector organizations should establish continuity programs that meet the general objectives of government continuity efforts and are tailored to their individual missions and circumstances. Identification of activities that support the Federal NEFs and government PMEFs will help the private sector develop effective continuity measures and programs. Continued performance of the private sector's operations will, in certain circumstances, assure the health, safety, and welfare needs of citizens and clients, maintain financial stability, and facilitate rapid and effective response to and recovery from the domestic consequences of an attack or other incident. Redundant, interoperable communications systems are a key component of a continuity program.

ROLES AND RESPONSIBILITIES

The responsibility for preparing and responding to emergencies is shared by government and the private sector. The private sector has critical roles in preparing for, responding to, and recovering from natural or manmade incidents or disasters. The large and diverse community of the private sector requires close coordination and integration with relevant government entities.

Requirements for effective private sector continuity programs track closely governmental objectives. Private sector leaders are encouraged to consider how the responsibilities outlined for governments in Chapter 4B apply to their activities. For example, private sector leaders should identify successors, put in place emergency delegations of authority, and plan for geographic dispersion of staff and infrastructure where appropriate. Both the safeguarding of vital resources, facilities, and records, and the acquisition of resources that permit continued operation will permit timely reconstitution and recovery from catastrophic emergencies and resumption of normal operations. Communications availability, redundancy and connectivity between and among key government leadership and the public are the responsibility of all entities with continuity obligations. Where appropriate, identification and training of personnel capable of implementing continuity programs should be part of private sector operations.

ACTIONS AND EXPECTATIONS

Department of Homeland Security

- Develop and promulgate continuity planning guidance for private sector critical infrastructure owners and operators. Guidance and planning for these organizations

should be integrated into the National Infrastructure Protection Plan and be supported by Critical Infrastructure/Key Resources (CI/KR) Coordinating Councils and Committees in accordance with guidance in HSPD-7;

- Make available continuity planning and exercise funding, in the form of grants as provided by law, to the private sector;

- Provide critical infrastructure assistance and support for the Nation's continuity of operations plans and programs in accordance with guidance in HSPD-7. Councils and committees established to support the National Infrastructure Protection Plan should be leveraged to support the activities of the DHS/FEMA regional and State level Continuity Working Groups (CWGs); and

- Invite the private sector to participate in government training and exercises, where appropriate.

Federal Intelligence and Law Enforcement Communities

- Provide intelligence to the private sector as appropriate and using official processes and communications methods.

Private Sector Critical Infrastructure Owners and Operators

The Federal Government, in conjunction with State and local governments, is extremely dependent on private sector leaders, especially during a crisis. The private sector owns and operates our Nation's communications backbone, energy infrastructure, financial networks, and other key components of our daily lives. Citizens and government are dependent on the owners and operators who make these pillars of our lives work on a daily basis.

Private sector organizations are encouraged to consider the following recommendations:

- Appoint a senior accountable official to be responsible for planning and implementation of continuity programs for the organization;

- Establish a continuity plan and program that ensures the performance of critical infrastructure essential functions and services during an emergency until normal operations can be resumed;

- Develop a vital resources, facilities, and records program that ensures these are safeguarded and that there is official access to them. Develop and implement training to support this program;

- Develop procedures for the acquisition of resources necessary for continuity operations on an emergency basis;

- Develop succession orders and preplanned devolution of authorities that ensure the emergency delegation of authority when necessary;

- Provide for the availability and redundancy of critical communications capabilities at critical infrastructure sites in order to support connectivity between and among key government and private sector leadership, internal elements, other organizations, and the public;

- Provide intelligence to Federal intelligence and law enforcement agencies as appropriate using official processes and communications methods;

- Plan, program, and budget for continuity capabilities consistent with this *Implementation Plan*, and submit to DHS grant funding requests, as provided by law;

- Plan and conduct continuity tests, training, and exercises, independently or in concert with government entities, in order to prepare and evaluate program readiness and ensure adequacy and viability of continuity plans and communications systems;

- Participate in national infrastructure protection coordinating councils and committees as identified in the National Infrastructure Protection Plan, and provide representatives, as requested by DHS, to participate in DHS/FEMA Regional and State Continuity Working Groups; and
- Establish an organizational continuity working group.

NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/NSPD-51

HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD-20

Subject: National Continuity Policy

Purpose

(1) This directive establishes a comprehensive national policy on the continuity of Federal Government structures and operations and a single National Continuity Coordinator responsible for coordinating the development and implementation of Federal continuity policies. This policy establishes "National Essential Functions," prescribes continuity requirements for all executive departments and agencies, and provides guidance for State, local, territorial, and tribal governments, and private sector organizations in order to ensure a comprehensive and integrated national continuity program that will enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency.

Definitions

(2) In this directive:

(a) "Category" refers to the categories of executive departments and agencies listed in Annex A to this directive;

(b) "Catastrophic Emergency" means 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;

(c) "Continuity of Government," or "COG," means a coordinated effort within the Federal Government's executive branch to ensure that National Essential Functions continue to be performed during a Catastrophic Emergency;

(d) "Continuity of Operations," or "COOP," means an effort within individual executive departments and agencies to ensure that Primary Mission Essential Functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies;

(e) "Enduring Constitutional Government," or "ECG," means 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, to preserve the constitutional framework under which the Nation is governed and the capability of all three branches of government to execute constitutional responsibilities and provide for orderly succession, appropriate transition of leadership, and interoperability and support of the National Essential Functions during a catastrophic emergency;

(f) "Executive Departments and Agencies" means the executive departments enumerated in 5 U.S.C. 101, independent establishments as defined by 5 U.S.C. 104(1), Government corporations as defined by 5 U.S.C. 103(1), and the United States Postal Service;

(g) "Government Functions" means the collective functions of the heads of executive departments and agencies as defined by statute, regulation, presidential direction, or other legal authority, and the functions of the legislative and judicial branches;

(h) "National Essential Functions," or "NEFs," means that subset of Government Functions that are necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through COOP and COG capabilities; and

(i) "Primary Mission Essential Functions," or "PMEFs," means those Government Functions that must be performed in order to support or implement the performance of NEFs before, during, and in the aftermath of an emergency.

Policy

(3) 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.

Implementation Actions

(4) Continuity requirements shall be incorporated into daily operations of all executive departments and agencies. As a result of the asymmetric threat environment, adequate warning of potential emergencies that could pose a significant risk to the homeland might not be available, and therefore all continuity planning shall be based on the assumption that no such warning will be received. Emphasis will be placed upon geographic dispersion of leadership, staff, and infrastructure in order to increase survivability and maintain uninterrupted Government Functions. Risk management principles shall be applied to ensure that appropriate operational readiness decisions are based on the probability of an attack or other incident and its consequences.

(5) The following 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:

(a) Ensuring the continued functioning of our form of government under the Constitution, including the functioning of the three separate branches of government;

(b) Providing leadership visible to the Nation and the world and maintaining the trust and confidence of the American people;

(c) 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;

(d) Maintaining and fostering effective relationships with foreign nations;

(e) 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;

(f) Providing rapid and effective response to and recovery from the domestic consequences of an attack or other incident;

(g) Protecting and stabilizing the Nation's economy and ensuring public confidence in its financial systems; and

(h) Providing for critical Federal Government services that address the national health, safety, and welfare needs of the United States.

(6) The President shall lead the activities of the Federal Government for ensuring constitutional government. In order to advise and assist the President in that function, the Assistant to the President for Homeland Security and Counterterrorism (APHS/CT) is hereby designated as

the National Continuity Coordinator. The National Continuity Coordinator, in coordination with the Assistant to the President for National Security Affairs (APNSA), without exercising directive authority, shall coordinate the development and implementation of continuity policy for executive departments and agencies. The Continuity Policy Coordination Committee (CPCC), chaired by a Senior Director from the Homeland Security Council staff, designated by the National Continuity Coordinator, shall be the main day-to-day forum for such policy coordination.

(7) For continuity purposes, each executive department and agency is assigned to a category in accordance with the nature and characteristics of its national security roles and responsibilities in support of the Federal Government's ability to sustain the NEFs. The Secretary of Homeland Security shall serve as the President's lead agent for coordinating overall continuity operations and activities of executive departments and agencies, and in such role shall perform the responsibilities set forth for the Secretary in sections 10 and 16 of this directive.

(8) The National Continuity Coordinator, in consultation with the heads of appropriate executive departments and agencies, will lead the development of a National Continuity Implementation Plan (Plan), which shall include prioritized goals and objectives, a concept of operations, performance metrics by which to measure continuity readiness, procedures for continuity and incident management activities, and clear direction to executive department and agency continuity coordinators, as well as guidance to promote interoperability of Federal Government continuity programs and procedures with State, local, territorial, and tribal governments, and private sector owners and operators of critical infrastructure, as appropriate. The Plan shall be submitted to the President for approval not later than 90 days after the date of this directive.

(9) Recognizing that each branch of the Federal Government is responsible for its own continuity programs, an official designated by the Chief of Staff to the President shall ensure 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.

(10) Federal Government COOP, COG, and ECG plans and operations shall be appropriately integrated with the emergency 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 to prevent redundancies and conflicting lines of authority. The Secretary of Homeland Security shall coordinate the integration of Federal 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) Continuity requirements for the Executive Office of the President (EOP) and executive departments and agencies shall include the following:

(a) 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;

(b) 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;

(c) Vital resources, facilities, and records must be safeguarded, and official access to them must be provided;

(d) Provision must be made for the acquisition of the resources necessary for continuity operations on an emergency basis;

(e) 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;

(f) Provision must be made for reconstitution capabilities that allow for recovery from a catastrophic emergency and resumption of normal operations; and

(g) 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.

(12) In order to provide a coordinated response to escalating threat levels or actual emergencies, the Continuity of Government Readiness Conditions (COGCON) system establishes executive branch continuity program readiness levels, focusing on possible threats to the National Capital Region. The President will determine and issue the COGCON Level. Executive departments and agencies shall comply with the requirements and assigned responsibilities under the COGCON program. During COOP activation, executive departments and agencies shall report their readiness status to the Secretary of Homeland Security or the Secretary's designee.

(13) The Director of the Office of Management and Budget shall:

(a) Conduct an annual assessment of executive department and agency continuity funding requests and performance data that are submitted by executive departments and agencies as part of the annual budget request process, in order to monitor progress in the implementation of the Plan and the execution of continuity budgets;

(b) In coordination with the National Continuity Coordinator, issue annual continuity planning guidance for the development of continuity budget requests; and

(c) Ensure that heads of executive departments and agencies prioritize budget resources for continuity capabilities, consistent with this directive.

(14) The Director of the Office of Science and Technology Policy shall:

(a) Define and issue minimum requirements for continuity communications for executive departments and agencies, in consultation with the APHS/CT, the APNSA, the Director of the Office of Management and Budget, and the Chief of Staff to the President;

(b) Establish requirements for, and monitor the development, implementation, and maintenance of, a comprehensive communications architecture to integrate continuity components, in consultation with the APHS/CT, the APNSA, the Director of the Office of Management and Budget, and the Chief of Staff to the President; and

(c) Review quarterly and annual assessments of continuity communications capabilities, as prepared pursuant to section 16(d) of this directive or otherwise, and report the results and recommended remedial actions to the National Continuity Coordinator.

(15) An official designated by the Chief of Staff to the President shall:

(a) Advise the President, the Chief of Staff to the President, the APHS/CT, and the APNSA on COGCON operational execution options; and

(b) Consult with the Secretary of Homeland Security in order to ensure synchronization and integration of continuity activities among the four categories of executive departments and agencies.

(16) The Secretary of Homeland Security shall:

(a) Coordinate the implementation, execution, and assessment of continuity operations and activities;

(b) Develop and promulgate Federal Continuity Directives in order to establish continuity planning requirements for executive departments and agencies;

(c) Conduct biennial assessments of individual department and agency continuity capabilities as prescribed by the Plan and report the results to the President through the APHS/CT;

(d) Conduct quarterly and annual assessments of continuity communications capabilities in consultation with an official designated by the Chief of Staff to the President;

(e) Develop, lead, and conduct a Federal continuity training and exercise program, which shall be incorporated into the National Exercise Program developed pursuant to Homeland Security Presidential Directive-8 of December 17, 2003 ("National Preparedness"), in consultation with an official designated by the Chief of Staff to the President;

(f) Develop and promulgate continuity planning guidance to State, local, territorial, and tribal governments, and private sector critical infrastructure owners and operators;

(g) Make available continuity planning and exercise funding, in the form of grants as provided by law, to State, local, territorial, and tribal governments, and private sector critical infrastructure owners and operators; and

(h) As Executive Agent of the National Communications System, develop, implement, and maintain a comprehensive continuity communications architecture.

(17) The Director of National Intelligence, in coordination with the Attorney General and the Secretary of Homeland Security, shall produce a biennial assessment of the foreign and domestic threats to the Nation's continuity of government.

(18) The Secretary of Defense, in coordination with the Secretary of Homeland Security, shall provide secure, integrated, Continuity of Government communications to the President, the Vice President, and, at a minimum, Category I executive departments and agencies.

(19) Heads of executive departments and agencies shall execute their respective department or agency COOP plans in response to a localized emergency and shall:

(a) Appoint a senior accountable official, at the Assistant Secretary level, as the Continuity Coordinator for the department or agency;

(b) Identify and submit to the National Continuity Coordinator the list of PMEFs for the department or agency and develop continuity plans in support of the NEFs and the continuation of essential functions under all conditions;

(c) Plan, program, and budget for continuity capabilities consistent with this directive;

(d) Plan, conduct, and support annual tests and training, in consultation with the Secretary of Homeland Security, in order to evaluate program readiness and ensure adequacy and viability of continuity plans and communications systems; and

(e) Support other continuity requirements, as assigned by category, in accordance with the nature and characteristics of its national security roles and responsibilities.

General Provisions

(20) This directive shall be implemented in a manner that is consistent with, and facilitates effective implementation of, provisions of the Constitution concerning succession to the Presidency or the exercise of its powers, and the Presidential Succession Act of 1947

(3 U.S.C.19), with consultation of the Vice President and, as appropriate, others involved. Heads of executive departments and agencies shall ensure that appropriate support is available to the Vice President and others involved as necessary to be prepared at all times to implement those provisions.

(21) This directive:

(a) Shall be implemented consistent with applicable law and the authorities of agencies, or heads of agencies, vested by law, and subject to the availability of appropriations;

(b) Shall not be construed to impair or otherwise affect (i) the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals, or (ii) the authority of the Secretary of Defense over the Department of Defense, including the chain of command for military forces from the President, to the Secretary of Defense, to the commander of military forces, or military command and control procedures; and

(c) Is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.

(22) Revocation. Presidential Decision Directive 67 of October 21, 1998 ("Enduring Constitutional Government and Continuity of Government Operations"), including all Annexes thereto, is hereby revoked.

(23) Annex A and the classified Continuity Annexes, attached hereto, are hereby incorporated into and made a part of this directive.

(24) Security. This directive and the information contained herein shall be protected from unauthorized disclosure, provided that, excepts for Annex A, the Annexes attached to this directive are classified and shall be accorded appropriate handling, consistent with applicable Executive Orders.

GEORGE W. BUSH

List of Department and Agency Categories (Annex A to NSPD-51/HSPD-20)

NATIONAL SECURITY PRESIDENTIAL DIRECTIVE-51 HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-20

NATIONAL CONTINUITY POLICY ANNEX A CATEGORIES OF DEPARTMENTS AND AGENCIES

(1) In accordance with NSPD-51/HSPD-20, National Continuity, Federal departments and agencies are assigned to one of four categories commensurate with their COOP/COG/ECG responsibilities during an emergency. These categories shall be used for continuity planning, communications requirements, emergency operations capabilities and other related requirements.

(2) Category I, Federal departments and agencies:

a. Department of State
b. Department of the Treasury
c. Department of Defense, including U.S. Army Corps of Engineers
d. Department of Justice, including the Federal Bureau of Investigation
e. Department of Health and Human Services
f. Department of Transportation
g. Department of Energy
h. Department of Homeland Security, including
    a. Federal Emergency Management Agency
    b. United States Secret Service
    c. National Communications Systemi.
i. Office of the Director of National Intelligence
j. Central Intelligence Agency

(3) Category II, Federal departments and agencies:

a. Department of Interior
b. Department of Agriculture
c. Department of Commerce
d. Department of Labor
e. Department of Housing and Urban Development
f. Department of Education
g. Department of Veterans Affairs
h. Environmental Protection Agency
i. Federal Communications Commission
j. Federal Reserve System
k. General Services Administration
l. National Archives and Records Administration
m. Nuclear Regulatory Commission
n. Office of Personnel Management
o. Social Security Administration
p. United States Postal Service

(4) Category III,

a. Commodity Futures Trading Commission
b. Export-Import Bank of the United States
c. Farm Credit Administration
d. Federal Deposit Insurance Corporation
e. Federal Mediation and Conciliation Service
f. National Aeronautics and Space Administration
g. National Credit Union Administration
h. National Labor Relations Board
i. National Science Foundation
j. Railroad Retirement Board
k. Security and Exchange Commission
l. Small Business Administration
m. Tennessee Valley Authority

(5) Category IV,

All executive branch organizations, including all commission, boards, bureaus, and members of the Small Agency Council, not otherwise identified in Categories I, II, or III.

Glossary of Terms

For the purposes of the *National Continuity Policy Implementation Plan*:

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 System
CCA	Continuity Communications Architecture
CI/KR	Critical Infrastructure and Key Resources
COG	Continuity of Government
COGCON	Continuity of Government Readiness Conditions
COOP	Continuity of Operations
CPCC	White House Homeland Security Council Continuity Policy Coordination Committee
CWG	Continuity Working Group
D/A	Departments and Agencies of the Federal Executive Branch
DEFCON	Defense Readiness Conditions
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOD	Department of Defense
EAS	Emergency Alert System
ECG	Enduring Constitutional Government

ESF	Emergency Support Function
FCC	Federal Communications Commission
FCD	Federal Continuity Directive
FEA	Federal Executive Associations
FEB	Federal Executive Board
FEMA	Federal Emergency Management Agency
FOC	FEMA Operations Center
FPCON	Department of Defense Force Protection Conditions
GSA	General Services Administration
HSAS	Homeland Security Advisory System
HSC	White House Homeland Security Council
HSDN	Homeland Security Data Network
HSEEP	Homeland Security Exercise and Evaluation Program
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
IAB	Interagency Board
IMPT	Department of Homeland Security Incident Management Planning Team
IPAWS	Integrated Public Alert Warning System
IT	Information Technology
JFO	Joint Field Office
MEF	Mission Essential Function
NARA	National Archives and Records Administration
NAWAS	National Alert Warning System
NCC	National Continuity Coordinator
NCCC	National Command and Coordination Capability

NCR	National Capital Region
NCS	National Communications System
NEEP	National Exercise and Evaluation Program
NEP	National Exercise Program
NEF	National Essential Function
NFG	Non-Federal Governments, including State, local, territorial, and tribal governments
NICC	National Infrastructure Coordinating Center
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Program
NOAA	National Oceanic and Atmospheric Administration
NOC	Department of Homeland Security National Operations Center
NRCC	Department of Homeland Security National Response Coordinating Center
NRP	National Response Plan
NSC	National Security Council
NSPD-51/HSPD-20	National Security Presidential Directive-51 and Homeland Security Presidential Directive-20.
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSTP	Office of Science and Technology Policy
PMEF	Primary Mission Essential Function
RRCC	Regional Response Coordination Centers
RRS	Readiness Reporting System
SAC	Small Agency Council
TT&E	Test, Training, and Exercise
WAWAS	Washington Metropolitan Area Warning System

DEFINITION OF TERMS

Alternate facilities – Locations, other than the primary facility, used to carry out essential functions, particularly in a continuity situation.

Biennial Continuity Assessments – An evaluation every two years of a department or agencies cumulative, integrated Continuity Capability.

Business Impact Analysis – A method of identifying the effects of failing to perform a function or requirement.

Business Process Analysis – A method of examining, identifying, and mapping the functional processes, workflows, activities, personnel expertise, systems, data, and facilities inherent to 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 – Refers to the categories of executive departments and agencies listed in Annex A to NSPD-51/HSPD-20 and Appendix B to this *Implementation Plan*.

COGCON – The Continuity of Government Readiness Condition system is a means to establish, measure, and report the readiness of executive branch continuity programs independent of other Federal Government readiness systems. (See Appendix D for a detailed matrix.)

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.

Continuity Capability – The ability of an organization to continue performance of Essential Functions, utilizing Continuity of Operations and Continuity of Government programs and integrated, day-to-day operations with a primary goal of ensuring the preservation of our form of government under the Constitution and the continuing performance of National Essential Functions under all conditions. Built from the foundation of continuity planning and continuity program management, the key pillars of 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 the executive branch departments and agencies at the Assistant Secretary (or equivalent) level.

Continuity of Government (COG) – A coordinated effort within the Federal Government's executive branch to ensure that National Essential Functions continue to be performed during a Catastrophic Emergency.

Continuity of Operations (COOP) – An effort within individual executive departments and agencies to ensure that Primary Mission Esse-

tial Functions continue to be performed during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.

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 System – The Corrective Action Program (CAP) System is a web-based application that allows Federal, State, and local emergency response and homeland security officials to track and analyze Improvement Plans. The Department of Homeland Security is developing this system as part of a larger effort to systematically translate Homeland Security Exercise and Evaluation Program (HSEEP) outputs—including findings, areas for improvement, recommendations, lessons learned, and best practices—into meaningful inputs for homeland security plans, programs, and budgets.

Delegation of authority – Identification, by position, of the authorities for making policy determinations and decisions at headquarters, field levels, and all other organizational locations. Generally, pre-determined delegations of authority will take effect when normal channels of direction are disrupted and terminate when these channels have resumed.

Devolution of authority – The passing of an unexercised right, devolution of authority is an essential planning requirement for departments and agencies manifested as a formal list of personnel who are pre-delegated the authority and responsibility to assume leadership of organizational elements within a department or agency with the approval of the department or agency head.

"Dirty bomb" – A type of radiological dispersal device (RDD) that combines a conventional explosive with radioactive material.

Emergency Alert System (EAS) – A national communications network and public warning system started in 1994 that replaced the Emergency Broadcast System jointly administered by the Federal Communications Commission, FEMA, and the National Weather Service. The System requires broadcasters, cable television systems, wireless cable systems, satellite digital audio radio service (SDARS) providers and, effective in May 2007, direct broadcast satellite (DBS) service providers to provide the communications capability to the President to address the American public during a national emergency. The system also may be used by state and local authorities to deliver important emergency information such as AMBER alerts and weather information targeted to a specific area.

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, to preserve the constitutional framework under which the Nation is governed and the capability of all three branches of government to execute constitutional responsibilities and provide for orderly succession, appropriate transition of leadership, and interoperability and support of the National Essential Functions during a catastrophic emergency.

Essential Functions – The critical activities that are performed by organizations, especially after a disruption of normal activities. There are three categories of essential functions: National Essential Functions (NEFs), Primary Mission Essential Functions (PMEFs), and Mission Essential Functions (MEFs).

Executive Departments and Agencies – The executive departments enumerated in 5 U.S.C. 101, independent establishments as defined by 5 U.S.C. 104(1), Government corporations as defined by 5 U.S.C. 103(1), and the United States Postal Service.

Facilities – Locations where leadership and staffs may operate. Leadership and staff may be co-located in one facility or dispersed through many locations, connected virtually through communications systems. Facilities must be able to provide survivable protection and enable continued, endurable operations.

Federal Continuity Directive (FCD) – A document developed and promulgated by DHS, in coordination with the CAG and in consultation with the Continuity PCC, 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 primarily 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 partnership in government.

FEMA Operations Center (FOC) – A continuously operating entity of the Department of Homeland Security responsible for monitoring emergency operations and promulgating notification of changes to the COGCON status.

Government Functions – The collective functions of the heads of executive departments and agencies as defined by statute, regulation, presidential direction, or other legal authority, and the functions of the legislative and judicial branches.

Homeland Security Advisory System – A series of tools used by the Department of Homeland Security to provide guidance to the public on the status of our 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 Data Network (HSDN) – A communications system and IT infrastructure used by the Department of Homeland Security to streamline and merge classified networks into a single, integrated network which is being designed to become a major secure information thoroughfare joining together intelligence agencies, law enforcement, disaster management, and front-line disaster response organizations.

Homeland Security Exercise and Evaluation Program (HSEEP) – The NEP utilizes the HSEEP as the common methodology for exercises. HSEEP is a capabilities- and performance-based exercise program that provides standardized policy, doctrine, and terminology for the design, development, conduct, and evaluation of homeland security exercises. HSEEP also provides tools and resources to facilitate the management of self-sustaining homeland security exercise programs.

Homeland Security Information Bulletins – Guidance for Federal, State, local, and other governments; private sector organizations; and international partners concerned with our Nation's critical infrastructures that do not meet the timeliness, specificity, or significance thresholds of warning messages. Bulletins often include statistical reports, periodic summaries, incident response or reporting guidelines, common vulnerabilities and patches, and configuration standards or tools.

Homeland Security Information Network (HSIN) – A communications system and IT infrastructure used by the Department of Homeland Security to transmit sensitive but unclassified information. The HSIN serves as a nationwide information-sharing and collaboration tool and is intended to offer real-time chat and instant messaging capability as well as a document library that contains reports from multiple Federal, State, and local sources. HSIN features suspicious incident information and analysis of terrorist threats, tactics, and weapons. HSIN includes over 35 communities of interest, such as emergency management, law enforcement, counterterrorism, States, and private sector communities. Each community of interest has Web pages that are tailored for the community and contain general and community-specific news articles, links, and contact information. HSIN features include a document library, a discussion thread/bulletin board capability, and a chat tool among others.

Homeland Security Threat Advisories – Guidance provided to Federal, State, local, and other governments; private sector organizations; and international partners with actionable information about an incident involving, or a threat targeting, critical national networks, infrastructures, or key assets. The Threat Advisories includes products formerly named alerts, advisories, and sector notifications.

Homeland Security Threat Level System – A color-coded system used to communicate with public safety officials and the public at-large through a threat-based, color-coded system so that protective measures can be implemented to reduce the likelihood of impact of an attack.

Integrated Public Alert Warning System (IPAWS) – Pursuant to Executive Order 13407, IPAWS is a comprehensive DHS/FEMA program, in partnership with NOAA, the FCC, and other public and private stakeholders, begun in 2004 to improve public alert and warning. The system will deliver digitally-based alert and warning messages to radio and television stations, personal computers, cell phones and other consumer wireless devices. The System seeks to upgrade EAS, enhance NAWAS, and begin other pilot programs, among other initiatives for current technological options.

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

Joint Field Office (JFO) – The JFO is a temporary Federal facility established locally to provide a central point for Federal, State, local, and tribal executives with responsibility for incident oversight, direction, and/or assistance to effectively coordinate protection, prevention, preparedness, response, and recovery actions. The JFO utilizes the scalable organizational structure of the NIMS in the context of both pre-incident and post-incident management activities. The JFO organization adapts to the magnitude and complexity of the situation at hand, and incorporates the NIMS principles regarding span of control and organizational structure by utilizing the Operations, Planning, Logistics, and Finance/Administration Sections. Although the JFO uses an ICS structure, the JFO does not manage on-scene operations. Instead, the JFO focuses on providing support to on-scene efforts and conducting broader support operations that may extend beyond the incident site. When incidents impact multiple States or localities, multiple JFOs may be established. In these situations, one of the JFOs may be identified (typically in the most heavily impacted area) to serve as the primary JFO and provide strategic leadership and coordination for the overall incident management effort, as designated by the Secretary of Homeland Security.

Leadership – The senior decision-makers designated to head an organization (e.g., President, Cabinet Secretary, Governor, Chief Executive Officer, or manager). Ensuring survivable leadership is accomplished by physically protecting the person (sheltering in place or relocating away from the threat), as well as having a prioritized list of designated successors. The designation as a successor enables a person to act for and exercise the powers of the principal in the event of death, permanent disability, or resignation.

Mission Essential Functions – The limited set of department- and agency-level government functions that must be continued throughout, or resumed rapidly after, a disruption of normal activities.

National Alert Warning System (NAWAS) – Operated and maintained by FEMA, the NAWAS was originally created as part of the Civil Defense Act of 1950 in order to pass emergency information to the American public regarding an actual attack or an accidental missile launch against the United States. The NAWAS is available on a 24/7 basis as a non-secure, continuous, private line, telephone system and is used to convey warnings to Federal, State, and local governments, as well as the military and civil populations. Although the original mission of NAWAS was to warn of an enemy attack or missile launch, the Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1974 expanded the NAWAS mission to include warning for acts of terrorism, as well as natural and technological disasters and events. NAWAS is used by the National Oceanic and Atmospheric Administration (NOAA) to pass severe weather alerts as conditions develop as well and to pass critical sheltering information in the event these severe weather conditions materialize. There are currently approximately 2050 NAWAS drops (referred to as Warning points) across the Nation, to include Alaska, Hawaii, Puerto Rico, and the US Virgin Islands.

National Capital Region (NCR) – The National Capital Region was created pursuant to the National Capital Planning Act of 1952 (40 U.S.C. § 71). The Act defined the NCR as the District of Columbia; Montgomery and Prince George's Counties of Maryland; Arlington, Fairfax, Loudon, and Prince William Counties of Virginia; and all cities now or here after existing in Maryland or Virginia within the geographic area bounded by the outer boundaries of the combined area of said counties. The NCR includes the District of Columbia and eleven local jurisdictions in the State of Maryland and the Commonwealth of Virginia.

National Command and Coordination Capability (NCCC) – The NCCC is the means to provide the President and Vice President with the ability to respond deliberately and appropriately to any crisis. It includes responsive, reliable, survivable, and robust processes and systems to command, control, and coordinate operations among Federal, State, tribal, insular, and local governments, as required.

National Communications System (NCS) – An organization within DHS, the NCS assists the President, the National Security Council, the Director of OSTP, and the Director of OMB in (1) the exercise of the telecommunications functions and responsibilities and (2) the coordination of the planning for and provision of national security and emergency preparedness communications for the Federal Government under all circumstances, including crisis or emergency, attack, and recovery and reconstitution.

National Essential Functions (NEFs) – The eight functions and overarching responsibilities of the Federal Government to lead and sustain the Nation that the President and national leadership will focus on during a catastrophic emergency that, therefore, must be supported through continuity capabilities.

National Exercise and Evaluation Program (NEEP) – NEP utilizes the NEEP to evaluate homeland security-related exercises and make improvements for the future.

National Exercise Program (NEP) – HSPD-8 directed the establishment of the NEP under the leadership of the Secretary of Homeland Security. The NEP is the Nation's overarching exercise program formulated by the National Security Council/Homeland Security Council, and executed by the Federal Interagency. The NEP serves as the principal mechanism for examining the preparation of the Federal executive branch and adopting policy changes that might improve such preparation. The NEP is DHS's principal mechanism for training and exercising officials at all levels of government, as well as members of the private sector, and, at times, our international partners. The NEP has developed common policy and guidance and has established collaborative management processes and tools to link its partners and stakeholders nationwide. Lessons learned and peer-validated best practices identified through exercises and actual incidents are made available to the homeland security community.

National Incident Management System (NIMS) – HSPD-5 directed the Secretary of Homeland Security to develop and administer a National Incident Management System 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 the cause, size, or complexity. NIMS benefits include a unified approach to incident management; standard command and management structures; and 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.

National Preparedness Goal – A requirement of HSPD-8 to define "standards for preparedness assessments and strategies, and a system for assessing the Nation's overall preparedness to respond to major events, especially those involving acts of terrorism." The Goal establishes measurable priorities, targets, and a common approach to developing needed capabilities. The Goal includes seven priorities for national preparedness: two overarching priorities and five priorities to build specific capabilities.

The overarching priorities of the National Preparedness Goal are to:

- Implement the National Incident Management System and National Response Plan
- Expand regional collaboration and
- Implement the Interim National Infrastructure Protection Plan.

The priorities for specific capabilities are to:

- Strengthen information sharing and collaboration capabilities;
- Strengthen interoperable communications capabilities;
- Strengthen chemical, biological, radiation, nuclear, and explosive weapons (CBRNE) detection, response, and decontamination capabilities; and
- Strengthen medical surge and mass prophylaxis capabilities.

National Response Coordinating Center (NRCC) – An entity of DHS's National Operations Center (NOC) that monitors, on a 24/7 basis or as required, potential or developing incidents and supports the efforts of regional and field components, including coordinating the preparedness of national-level emergency response teams and resources; initiating mission assignments or reimbursable agreements to activate other Federal departments and agencies in coordination with the NOC and Regional Response Coordination Centers; and activating and deploying national-level specialized teams. In addition, the NOC/NRCC resolve Federal resource support conflicts and other implementation issues forwarded by Joint Field Offices.

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.

Regional Response Coordination Center (RRCC) – The RRCC is a standing facility operated by DHS/FEMA that coordinates regional response efforts, establishes Federal priorities, and implements local Federal program support until a JFO is established in the field and/or other key DHS incident management officials can assume their NRP coordination responsibilities. The RRCC establishes communications with the affected State Emergency Operations Center (EOC) and the NOC-NRCC, coordinates deployment of the Emergency Response Team–Advance Element (ERT-A) to field locations, assesses damage information, develops situation reports, and issues initial mission assignments.

Staff – Those personnel, both senior and core personnel, that provide the leadership advice, recommendations, and the functional support necessary to continue essential operations.

Target Capabilities List – A component of the National Preparedness Goal from HSPD-8 which describes and sets targets for the capabilities required to achieve the four homeland security mission areas: Prevent, Protect, Respond, and Recover. The List defines and provides the basis for assessing preparedness. It also establishes national targets for the capabilities to prepare the Nation for major all-hazards events, such as those defined by the National Planning Scenarios. The current version of the TCL contains 37 core capabilities.

Washington Metropolitan Area Warning System (WAWAS) – The Washington Area Warning System (WAWAS), is a portion of the NAWAS, but is not tied directly to the NAWAS. It is operated and maintained by the FEMA Operations Center. While the NAWAS is nationwide, the WAWAS is dedicated to the Washington, DC, metropolitan area. On a day-to-day basis, the DC Office of Emergency Management manages the WAWAS due to the amount of local information disseminated across the system. OPM uses the WAWAS to pass duty information to the various Federal departments and agencies located in the Washington, DC, area in the event of bad weather or other business affecting government operations.

COGCON Matrix

Readiness Level	Department & Agency (D/A)		
	Operations	Staffing Level	Time to Transition to Successive Stages
COGCON 4	• 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	• 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	• Continuity plan is fully operational within 12 hours
COGCON 3	• 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)	• 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	• Continuity plan is fully operational within 8 hours • 4 hours to COGCON 2
COGCON 2	• 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	• Deploy sufficient staff to alternate operating facility(ies) to allow activation with 4 hours notice	• Continuity plan is fully operational within 4 hours • 4 hours to COGCON 1
COGCON 1	• 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	• Deploy sufficient staffing to alternate operating facility(ies) to perform essential functions with no notice	• Agency headquarters continuity plan activated immediately and report operational status within two hours

	Continuity Capability		
	Communications	**Succession**	**Impact on Departments & Agencies**
	• Test all internal agency communications capabilities between normal operating locations (HQ and other) and alternate operating facility(ies) no less than quarterly • Test all communications capabilities at all alternate operating facility(ies) with applicable interagency partners no less than quarterly	• No special measures to protect or track the location of agency leadership and successors • Ensure delegations of authority to lead departments and agencies are in place for senior personnel located outside of the National Capital Region	• No additional requirements
	• Conduct at least one additional internal agency communications test between normal operating locations (HQ and other) and alternate operating facility(ies) within 24 hours	• Track the locations of agency leaders and their successors on daily basis	• Additional staff time for communications testing and tracking agency leadership • Potential shorter response times for basic staffing of alternate facility(ies)
	• 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	• 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	• 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)
	• 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	• 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)	• Some agency leaders work from alternate facility(ies) • Significant number of staff are required to work from alternate location(s)

Selected Continuity Authorities

Document Name	Effective Date	Description
Defense Production Act	9/1950	Provides primary authority to ensure the timely availability of resources for national defense and civil emergency preparedness and response.
Executive Order 12472	4/1984	Assigns national security and emergency preparedness telecommunications functions.
Executive Order 12656 NOTE: Upon the development of department and agency MEFs and PMEFs, which will replace the specific functions assigned to heads of departments and agencies in EO 12656, it is anticipated that a recommendation to revoke EO 12656 entirely will be sent to the President.	11/1988	Assigns responsibilities to each Federal agency for national security and emergency preparedness.
Federal Preparedness Circular 60	7/1999	Provides guidance to Federal executive branch departments and agencies for use in developing viable and executable contingency plans for the continuity of operations.
Federal Preparedness Circular 65	6/2004	Provides guidance to Federal executive branch departments and agencies for use in developing viable and executable contingency plans for the continuity of operations.
Homeland Security Presidential Directive-1 (HSPD-1)	10/2001	Provides for the organization and operation of the Homeland Security Council.
Homeland Security Presidential Directive-3 (HSPD-3)	3/2002	Provides for a Homeland Security Advisory System to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people.

Document Name	Effective Date	Description
Homeland Security Presidential Directive-5 (HSPD-5)	2/2003	Enhances the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system.
Homeland Security Presidential Directive-7 (HSPD-7)	12/2003	Establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.
Homeland Security Presidential Directive-8 (HSPD-8)	12/2003	Establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities.
Homeland Security Presidential Directive-9 (HSPD-9)	2/2004	Establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.
Homeland Security Presidential Directive-12 (HSPD-12)	8/2004	Establishes a policy for a Common Identification Standard for Federal employees and contractors.
Homeland Security Presidential Directive-20 / National Security Presidential Directive-51 (HSPD-20/NSPD-51)	5/2007	Establishes a comprehensive national policy on the continuity of Federal Government structures and operations and a single National Continuity Coordinator responsible for coordinating the development and implementation of Federal continuity policies; establishes "National Essential Functions"; prescribes continuity requirements for all executive departments and agencies; and provides guidance for State, local, territorial, and tribal governments, and private sector organizations in order to ensure a comprehensive and integrated national continuity program that will enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency.
National Infrastructure Protection Plan (NIPP)	2006	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.
National Response Plan (currently under review)	Last updated 5/2006	Provides the structure and mechanisms for the coordination of Federal support to State, local, and tribal incident managers and for exercising direct Federal authorities and responsibilities.

Document Name	Effective Date	Description
National Security Presidential Directive-1 (NSPD-1)	2/2001	Provides for the organization of the National Security Council.
National Security Strategy	3/2006	Promotes freedom, justice, and human dignity; confronts the challenges of the threat of pandemic disease, proliferation of weapons of mass destruction, terrorism, human trafficking, and natural disasters; and emphasizes effective multinational efforts to solve these problems.
National Strategy for Homeland Security (currently under review)	7/2002	Mobilize and organizes the Nation to secure the U.S. homeland from terrorist attacks; establishes a foundation upon which to organize efforts; and provides initial guidance to prioritize the work ahead.
National Strategy for Pandemic Influenza	11/2005	Provides a framework for future U.S. Government planning efforts to address the pandemic threat that is consistent with the *National Security Strategy* and the *National Strategy for Homeland Security*.
National Strategy for Pandemic Influenza Implementation Plan	5/2006	Represents a comprehensive effort by the Federal Government to identify the critical steps that must be taken immediately and over the coming months and years to address the threat of an influenza pandemic; assigns specific responsibilities to departments and agencies across the Federal Government; and includes measures of progress and timelines for implementation to ensure the preparedness objectives are met.
National Strategy for the Physical Protection of Critical Infrastructures and Key Assets	2/2003	Serves as a critical bridge between the *National Strategy for Homeland Security* and a national protection plan to be developed by the Department of Homeland Security. The strategic objectives that underpin the national infrastructure and key asset protection effort include: • Identifying and assuring the protection of those infrastructure and assets we deem most critical; • Providing timely warning and assuring the protection of those infrastructures and assets that face a specific, imminent threat; and • Assuring the protection of other infrastructures and assets that may become targets over time by pursuing specific initiatives and enabling a collaborative environment between the public and private sector.
The National Strategy to Secure Cyberspace	2/2003	Engages and empowers Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact.
Presidential Succession Act of 1947 (3 U.S.C. 19)	6/1948	Lays out procedures for succession to the Office of the President and Office of the Vice President.

Document Name	Effective Date	Description
Stafford Act	1988	Establishes programs and processes for the Federal Government to provide disaster and emergency assistance to States, local governments, tribal nations, individuals, and qualified private nonprofit organizations.
Twenty-Fifth Amendment	Ratified 2/1967	Clarifies a provision of the Constitution regarding succession to the Presidency, and establishes procedures both for filling a vacancy in the Office of the Vice President as well as responding to Presidential disabilities.

Continuity Requirements and Metrics

Paragraph 11 of the *National Continuity Policy* (NSPD-51/HSPD-20) identifies the continuity requirements for the Executive Office of the President and executive branch departments and agencies. This *Implementation Plan* requires department and agency heads to take the following action:

> *Task 5. Within 30 days and annually thereafter, submit a report to the NCC certifying that the department or agency has a continuity capability plan that includes the items in Paragraph 11 of NSPD-51/HSPD-20.*

From the list of continuity requirements (see below), department and agency heads shall use the key questions and metrics guidance below to certify 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 *(Provide justification including quantitative and/or qualitative data to show you have met the requirement <OR> identify steps you will take to do so.)*
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;	• 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?	• 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;	• 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?	• 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;	• 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?	• 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 *(Provide justification including quantitative and/or qualitative data to show you have met the requirement <OR> identify steps you will take to do so.)*
4.	Provision must be made for the acquisition of the resources necessary for continuity operations on an emergency basis;	• Have you identified emergency continuity resources? • Do you have agreements/ contracts to acquire emergency continuity resources?	• 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;	• Do you have critical communications capability at your alternate site(s)? • Do you have redundant communications capability at your alternate site(s)?	• 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	• What is your plan to ensuring your reconstitution capability?	• 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.	• Have you identified, trained, and prepared personnel to relocate to alternate sites to continue PMEFs?	• Verify that staff are identified, trained, and prepared to relocate to alternate sites.

Stoplight Scoring System

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

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

The NCC and the HSC, in coordination with DHS, will work with departments and agencies to further define continuity standards using a consistent Continuity Capability Scoring System to allow continuing assessment of improvement in continuity capability.

Implementation Plan Requirements and Deadlines Matrix

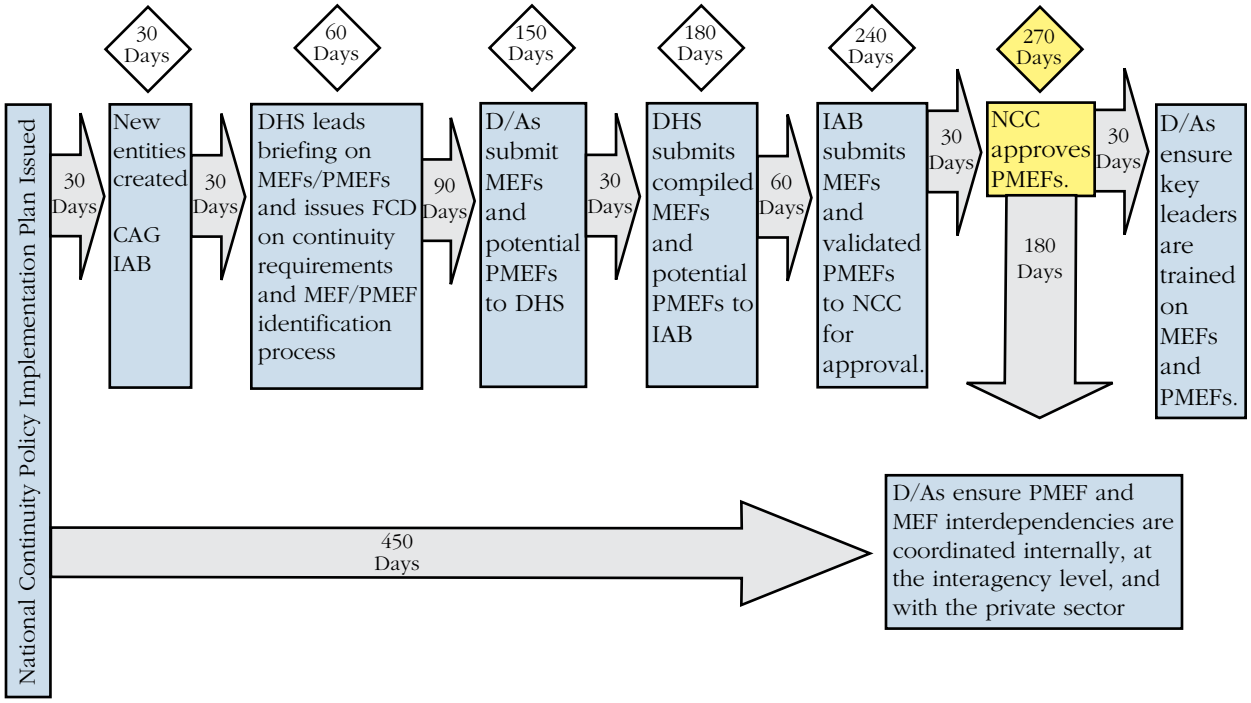
Responsible Party	Required Action	First Due Date	Subsequent Due Date
National Continuity Coordinator / APHS/CT	1. On an ongoing basis, provide continuity policy coordination among all departments and agencies, monitor performance, and report to the President as appropriate.	On an ongoing basis	
	2. As required, coordinate revision of the NEFs and department and agency PMEFs and MEFs.	As required	
	3. As required, ensure that the Homeland Security Council (HSC) staff conducts meetings of the CPCC.	As required	
	4. Within 30 days, establish a Continuity Advisory Group (CAG).	Within 30 days	
	5. Within 30 days, establish an Interagency Board (IAB) to review PMEFs.	Within 30 days	
	6. Within 30 days of IAB review, consider identified PMEFs for validation and approval.	Within 30 days of IAB review	
	7. Within 90 days, coordinate with FEMA in developing a continuity assessment tool for the departments and agencies to measure continuity readiness against requirements contained in NSPD-51/HSPD-20 and report the continuity assessment results to the President.	Within 90 days	
	8. Within the annual budget process and on an ongoing basis, assist OMB and departments and agencies with continuity budget development and prioritization, including long-term equipment life cycle replacements and upgrades.	Within the annual budget process and on an ongoing basis	
	9. On an ongoing basis, ensure coordination of continuity acquisition-functions with DHS and the General Services Administration (GSA).	On an ongoing basis	
	10. On an ongoing basis, coordinate the integration of national continuity test, training, and exercise programs.	On an ongoing basis	
	11. Annually submit 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 goverments and the private sector to perform the NEFs and achieve common continuity goals.		Annually
Secretary of Homeland Security	1. On an ongoing basis, serve 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 perform the responsibilities set forth in NSPD-51/HSPD-20 and in HSPD-5.	On an ongoing basis	

Responsible Party	Required Action	First Due Date	Subsequent Due Date
Secretary of Homeland Security	2. On an ongoing basis, ensure 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 and incident management activities.	On an ongoing basis	
	3. On an ongoing basis, ensure 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.	On an ongoing basis	
	4. On an ongoing basis, ensure that DHS makes available continuity planning and exercise funding in the form of grants as provided by law, to State, local, territorial, and tribal governments.	On an ongoing basis	
	5. On an ongoing basis, ensure 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 Critical Infrastructure and Key Resources (CI/KR) on continuity priorities and implementation guidelines.	On an ongoing basis	
	6. Not less than quarterly, conduct assessments of continuity communications capabilities in consultation with an official designated by the Chief of Staff to the President.		Not less than quarterly
	7. Within 60 days, establish a familiarization briefing on MEF and PMEF identification for department and agency Continuity Coordinators (Assistant Secretary-level).	Within 60 days	
	8. Within 60 days, in coordination with the Continuity PCC, issue a Federal Continuity Directive on Continuity Requirements, to include the formalized process for departments and agencies to identify MEFs, and revise through annual, or as needed, Directives thereafter.	Within 60 days	Annually or as needed
	9. Within 60 days, in coordination with the Continuity PCC, issue a Federal Continuity Directive on the formalized process for department and agency submission of potential PMEFs that are consistent and supportive of the NEFs. • Include a standardized checklist to allow departments and agencies to assess their PMEFs through a risk management process; • Include guidance on how the PMEFs link to/support NEF(s); and • Include guidance on impact statements if a specific PMEF is not conducted.	Within 60 days	
	10. Within 30 days after submission of department and agency MEFs and potential PMEFs, compile submissions and provide them to the NCC for IAB review and validation.	Within 30 days of submission	
	11. Within one year and annually thereafter, update training courses for department and agency continuity planners on the identification and development of PMEFs and MEFs, in addition to maintaining ongoing continuity training courses.	Within 1 year	Annually thereafter

Responsible Party	Required Action	First Due Date	Subsequent Due Date
Secretary of Homeland Security	12. 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), provide the Director of OSTP and 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.	Within 30 days after receipt of technical requirements	
	13. Within 90 days after receipt of technical requirements from OSTP, through the NCS, develop, implement, and begin maintenance of a comprehensive CCA.	Within 90 days after receipt of technical requirements	Ongoing
	14. On an annual basis, develop, lead, and conduct an integrated (COOP and COG) continuity training exercise, incorporated into the National Exercise Program, and report the results to the NCC.	On an annual basis	
	15. On an as needed basis, revise and promulgate integrated continuity planning guidance to non-Federal Governments and others as appropriate.	On an as needed basis	
	16. On an as needed basis, provide critical infrastructure assistance and support in accordance with HSPD-7 and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.*	On an as needed basis	
	17. On an as needed basis, provide cybersecurity assistance and support in accordance with HSPD-7 and the *National Strategy to Secure Cyberspace.*	On an as needed basis	
	18. Develop regional and state level Continuity Working Groups to, at a minimum, conduct annual continuity conferences to address joint Federal and non-Federal Government continuity planning and other elements of a viable continuity program.	As required and annually	
Executive Branch D/A Heads	1. On an ongoing basis, ensure performance of department or agency Primary Mission Essential Functions.	On an ongoing basis	
	2. On an ongoing basis, incorporate continuity requirements into daily department and agency operations.	On an ongoing basis	
	3. On an ongoing basis, ensure the department or 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 and other essential functions.	On an ongoing basis	
	4. Within 30 days, appoint a senior accountable official, at the Assistant Secretary or equivalent level, as the Continuity Coordinator for the department or agency.	Within 30 days	Maintain role
	5. Within 30 days and annually thereafter, submit a report to the NCC certifying that the department or agency has a continuity capability plan that includes the items in Paragraph 11 of NSPD-51/HSPD-20 (see Box 12).	Within 30 days	Annually thereafter
	6. On an ongoing basis, consistent with sections 11(e) and 19(c) of NSPD-51/HSPD-20, plan, program, and budget for secure continuity communications capabilities.	On an ongoing basis	

Responsible Party	Required Action	First Due Date	Subsequent Due Date
Executive Branch D/A Heads	7. Within 90 days after DHS' guidance, review and revise MEFs and identify and submit potential PMEFs to the IAB.	Within 90 days of DHS' guidance	
	8. Within 30 days after validation of department and agency PMEFs and annually thereafter, ensure key leaders and support staff are provided familiarization training of department or agency PMEFs and MEFs.	Within 30 days of validation	Annually thereafter
	9. Within 180 days after validation of department and agency PMEFs, ensure PMEF and MEF interdependencies are coordinated internally, at the interagency level, and with private sector partners.	Within 180 days of validation	On an ongoing basis
	10. On an ongoing basis, participate in DHS's National Exercise Program.	On an ongoing basis	
	11. On an ongoing basis, incorporate OMB Circular A-11 guidance, or other OMB guidance on continuity as provided, when developing continuity budgets.	On an ongoing basis	
	12. As required, submit Continuity Readiness Reports, and other reports as requested, through the Readiness Reporting System.	As required, monthly, quarterly, and upon COOP activation	
Director of OMB	1. As necessary, in coordination with the NCC, issue continuity planning guidance for the development of continuity budget requests.		As necessary
	2. Annually conduct an assessment of executive department and agency continuity funding requests and performance data that are submitted by executive branch departments and agencies as part of the annual budget request process in order to monitor progress in the execution of this *Plan* and continuity budgets.		Annually
	3. Annually reconcile department and agency continuity funding requests and performance data with Continuity Readiness Reporting and annual continuity assessments compiled by FEMA.		Annually
Director of OSTP	1. Annually review and revise 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).		Annually review and revise as required
	2. Within 60 days, establish and chair a Continuity Communications Architecture Board (CCAB).	Within 60 days	
	3. Within 30 days after validation of PMEFs, distribute requirements for, and update as needed, a comprehensive Continuity Communications Architecture (CCA) in consultation with the APMS/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).	Within 30 days after validation of PMEFs	

Responsible Party	Required Action	First Due Date	Subsequent Due Date
Director of OSTP	4. On an ongoing basis, monitor 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).	On an ongoing basis	
	5. Quarterly and annually, review assessments of continuity communications capabilities and report the results and recommended remedial actions to the NCC.		Quarterly and annually
An official designated by the Chief of Staff to the President	1. On an ongoing basis, advise the President, Chief of Staff to the President, the APHS/CT, and the APNSA on COGCON operational execution options.	On an ongoing basis	
	2. On an ongoing basis, ensure 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.	On an ongoing basis	
	3. On an ongoing basis, consult with the Secretary of Homeland Security in order to ensure synchronization and integration of continuity activities among the four categories of executive departments and agencies.	On an ongoing basis	
Secretary of Defense	1. Within 60 days after the publication by DHS of the Continuity Communications Architecture implementation plan, identify the secure, integrated Continuity of Government communications for use by the President, the Vice President, and, at a minimum, Category I executive departments and agencies.	Within 60 days of the CCA implementation plan	
	2. Upon identification and implementation, continuously maintain the secure, integrated, Continuity of Government communications for the President, the Vice President, and, at a minimum, Category I executive branch departments and agencies.	Upon identification and implementation	Continuously
	3. Not less than quarterly, assist the Secretary of Homeland Security, and an official designated by the Chief of Staff to the President, with assessments of continuity communications capabilities.	Not less than quarterly	
	4. On an ongoing basis, assist DHS in conducting continuity training and exercises and in providing assistance during emergencies and disasters.	On an ongoing basis	
Director of National Intelligence	1. Every two years, produce an assessment for the NCC of the foreign and domestic threats to the Nation's Continuity of Government.		Every two years
	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.	On an ongoing basis	
	3. During emergencies and disasters, provide geospatial continuity operational support to DHS to assist in response and recovery operations.	During emergencies and disasters	
Secretary of Homeland Security	1. Within 90 days, coordinate with the APHS/CT in developing a continuity assessment tool for the departments and agencies to measure continuity readiness against requirements contained in NSPD-51/HSPD-20.	Within 90 days	
	2. Quarterly, ensure FEMA's Continuity Coordinator chairs meetings of the CAG and reports to the Continuity PCC.		Quarterly

Responsible Party	Required Action	First Due Date	Subsequent Due Date
Secretary of Homeland Security	3. Every two years, conduct department and agency assessments of continuity capabilities and report the results to the NCC.		Every two years
	4. On an ongoing basis, operate and maintain the Readiness Reporting System.	On an ongoing basis	
	5. On an as needed basis in coordination with the CAG and in consultation with the CPCC, develop and promulgate Federal Continuity Directives that establish continuity planning requirements, continuity plan templates, TT&E programs, and assessment criteria.	On an as needed basis	
	6. On an ongoing basis, ensure that the FEMA Operations Center (FOC) maintains 24-hour operations to ensure appropriate procedures for emergency operations.	On an ongoing basis	
Director of OPM	1. Within 120 days, develop and promulgate personnel guidance to support Federal executive branch continuity plans and programs.	Within 120 days	
	2. Within 120 days, establish telework guidance to support department and agency continuity programs.	Within 120 days	
	3. Within 120 days, in coordination with the Secretary of Homeland Security, provide guidance and coordinate with the Federal Executive Boards (FEB) to assist in facilitating planning meetings and exercises to develop effective continuity programs.	Within 120 days	
	4. On an ongoing basis, assist DHS in conducting continuity training, exercises, assessments, and other preparedness activities.	On an ongoing basis	
	5. Within 120 days, submit a report to the NCC on the possibility of creating an occupational specialty for continuity and an associated training program, and, if approved, work with FEMA to include the information in a Federal Continuity Directive.	Within 120 days	
Administrator of the General Services Administration	1. On an ongoing basis, coordinate the provision of executive branch facilities to support continuity operations and maintain the database for all department and agency alternate facilities.	On an ongoing basis	
	2. On an ongoing basis, facilitate a coordinated and seamless executive branch continuity infrastructure and provide and maintain a centralized procurement system for all department and agency continuity infrastructure requirements.	On an ongoing basis	
	3. On an ongoing basis, assist the Secretary of Homeland Security in conducting continuity tests, training, exercises, assessments, and other preparedness activities.	On an ongoing basis	
	4. During and in the aftermath of emergencies and disasters, assist the Secretary of Homeland Security and affected departments and agencies in their recovery and reconstitution.	During and in the aftermath of emergencies and disasters	
Chairman of the Small Agency Council	1. On an ongoing basis, in coordination with the Secretary of Homeland Security, provide a forum for development and integration of continuity policies and programs among the Federal Government organizations represented on the Council.	On an ongoing basis	
Federal Executive Associations	1. On an ongoing basis, provide assistance where practicable in coordinating continuity activities for FEA members.	On an ongoing basis	

MEF/PMEF Indentification Timeline