Continuity Guidance Circular 1 (CGC 1)

Continuity Guidance for Non-Federal Entities

(States, Territories, Tribal, and Local Government Jurisdictions and Private Sector Organizations)

January 21, 2009

FEMA

This page is intentionally left blank.

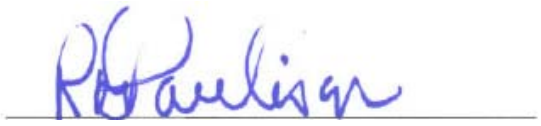
FEMA

The President issued the National Security Presidential Directive-51/Homeland Security Presidential Directive-20 (NSPD-51/HSPD-20) *National Continuity Policy* in May 2007 to establish and maintain a comprehensive and effective national continuity capability in order to ensure the preservation of our form of Government under the Constitution and the continuing performance of National Essential Functions under all conditions. In August 2007, the President approved the *National Continuity Policy Implementation Plan* to build upon the *Policy* and provide guidance to executive departments and agencies on appropriately identifying and carrying out their Primary Mission Essential Functions that support the eight National Essential Functions—the most essential functions necessary to lead and sustain the Nation during a catastrophic emergency.

To provide the operational guidance to implement this policy, the Department of Homeland Security, Federal Emergency Management Agency, in coordination with our non-federal partners, has developed Continuity Guidance Circular 1 (CGC 1), *Continuity Guidance for Non-Federal Entities.* The purpose of this guidance document is to provide direction for the development of continuity plans and programs for non-federal entities. Effective continuity planning and programs facilitate the performance of essential functions during all-hazards emergencies or other situations that may disrupt normal operations. The primary goal of continuity is the continuation of essential functions.

In this guidance document, the elements of a viable continuity capability are identified and discussed. These elements are critical to establishing and maintaining a comprehensive and effective continuity capability. Continuity programs and operations are good business practices that ensure critical services will be available to the Nation's citizens under all conditions.

The provisions of this guidance document are applicable for State, local, territorial and tribal governments and the private sector.



R. David Paulison
Administrator
Federal Emergency Management Agency

This page is intentionally left blank.

TABLE OF CONTENTS

This page is intentionally left blank.

CONTINUITY GUIDANCE CIRCULAR 1 (CGC 1)

Number	Date	Office
CGC 1	January 21, 2009	FEMA National Continuity Programs

TO: HEADS OF NON-FEDERAL ENTITIES

SUBJECT: CONTINUITY GUIDANCE FOR NON-FEDERAL ENTITIES

PURPOSE: This guidance document provides direction to non-federal entities for developing continuity plans and programs. Continuity planning facilitates the performance of essential functions during all-hazards emergencies or other situations that may disrupt normal operations. 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 National Essential Functions (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.

1. **APPLICABILITY AND SCOPE:** The provisions of this guidance document are applicable to all non-federal entities. The State, local, territorial and tribal governments, and the private sector are hereinafter referred to as "non-federal entities or organizations."

2. **SUPERSESSION:** The provisions of CGC 1 supersede: *Interim Guidance on Continuity of Operations Planning for State and Local Governments,* dated May 2004.

3. **AUTHORITIES:**
   See Annex Q – Authorities and References.

4. **REFERENCES:**
   See Annex Q – Authorities and References.

5. **POLICY:** It is the policy of the United States to maintain a comprehensive and effective continuity capability composed of Continuity of Operations (COOP) and Continuity of Government (COG) programs to ensure the preservation of our form of Government under the Constitution and the continuing performance of NEFs under all conditions (National Security Presidential Directive (NSPD)-51/Homeland Security Presidential Directive (HSPD)-20, *National Continuity Policy*). Continuity requirements must be incorporated into the daily operations of all agencies to ensure seamless and immediate continuation of Mission Essential Function (MEF)/Primary Mission Essential Function (PMEF) capabilities so that critical government functions and services remain available to the Nation's citizens.

Continuity planning is the good business practice of ensuring the execution of essential functions under all circumstances. Continuity includes all activities conducted by jurisdictions to ensure that their essential functions can be performed. This includes plans and procedures that delineate essential functions, specify succession to office and emergency delegation of authority, provide for the safekeeping of vital records and databases, identify alternate operating strategies, provide for continuity communications, and validate these capabilities through test, training, and exercise (TT&E) programs. Today's changing threat environment and the potential for no-notice emergencies, including localized acts of nature, accidents, technological system failures, and military or terrorist attack-related incidents, have increased the need for continuity capabilities and planning across all levels of government and the private sector.

6. <u>BACKGROUND</u>: Continuity planning is a fundamental responsibility of public institutions and private entities to our nation's citizens. Continuity planning facilitates the performance of essential functions during an emergency situation that disrupts normal operations and/or the timely resumption of normal operations once the emergency has ended. A strong continuity plan provides the organization with the means to address the numerous issues involved in performing essential functions and services during an emergency. Without detailed and coordinated continuity plans, and effective continuity programs to implement these plans, jurisdictions risk leaving our nation's citizens without vital services in what could be their time of greatest need.

The goal of continuity planning is to reduce the consequence of any disruptive event to a manageable level. The specific objectives of a particular organization's continuity plan may vary, depending on its mission and functions, its capabilities, and its overall continuity strategy. In general, continuity plans are designed to:

a. Minimize loss of life, injury, and property damage.
b. Mitigate the duration, severity, or pervasiveness of disruptions that do occur.
c. Achieve the timely and orderly resumption of essential functions and the return to normal operations.
d. Protect essential facilities, equipment, records, and assets.
e. Be executable with or without warning.
f. Meet the operational requirements of the respective organization. Continuity plans may need to be operational within minutes of activation, depending on the essential function or service, but certainly should be operational no later than 12-hours after activation.
g. Meet the sustainment needs of the respective organization. An organization may need to plan for sustained continuity operations for up to 30-days or longer, depending on resources, support relationships, and the respective continuity strategy adopted.
h. Ensure the continuous performance of essential functions and operations during an emergency, including those such as pandemic influenza that require additional considerations beyond traditional continuity planning.
i. Provide an integrated and coordinated continuity framework that takes into consideration other relevant organizational, governmental, and private sector continuity plans and procedures.

Responsibility for continuity planning resides with the highest level of management of the organization involved. The senior Elected Official or the administrative head of a State or local organization is ultimately responsible for the continuation of essential services during an emergency and for the related planning. Organizational responsibilities typically include the development of the strategic continuity vision and overarching policy, the appointment of key continuity personnel, and the development of a program budget that provides for adequate facilities, equipment, and training.

Organizational continuity planning cannot be approached in isolation. The effectiveness of one continuity plan is often dependent upon the execution of another organization's continuity plan as many agency functions rely on the availability of resources or functions controlled by another organization. Such interdependencies routinely occur between government and private sector organizations. Likewise, many government continuity plans are dependent upon private sector resources, especially in the area of critical infrastructure and key resources (CI/KR) support.

Effective implementation of continuity plans and programs requires the support of senior leaders and decision makers who have the authority to commit the organization and the necessary resources to support the programs. Emergency management officials are often responsible for developing or assisting in the development of continuity plans and programs for their jurisdictions. They are also available to assist in reestablishing essential functions and services during emergencies and disasters.

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

Pillars 1 and 2: People – Leadership and Staff

Continuity of leadership is critical to ensure continuity of essential functions. Organizations should 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 and other authorities to carry out their duties. Continuity of leadership during crisis, especially in the case of senior positions is important to reassure the Nation and give confidence to its citizens that the principal or appropriate successor is managing the crisis and ensuring the performance of essential functions. Leaders need to set priorities and keep focus.

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

Pillar 3: Communications and Technology

The ability to communicate is critical to daily operations and absolutely essential in a crisis. The Nation's domestic and international telecommunications resources, including commercial, private, and Government-owned services and facilities, are essential to support continuity plans and programs. All organizations should identify the communication requirements needed to perform their essential functions during both routine and continuity conditions. Communication systems and technology should be interoperable, robust, and reliable. Planners should consider the resilience of their systems to operate in disaster scenarios that may include power and other infrastructure problems.

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

Pillar 4: Facilities

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

The 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 should include all of the requirements and procedures needed to perform essential functions.

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

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

Continuity Program Management Cycle

A standardized continuity program management cycle ensures consistency across all continuity programs and supports the foundation and pillars that comprise the Nation's continuity capability. It establishes consistent performance metrics, prioritizes implementation plans, promulgates best practices, and facilitates consistent cross-agency continuity evaluations. Such a cyclic-based model that incorporates planning, training, evaluating, and the implementation of corrective actions, gives key leaders and essential personnel the baseline information, awareness, and experience necessary to fulfill their continuity program management responsibilities. The continuity program management cycle consists not only of its programmatic elements, but also should include the plans and procedures that support implementation of the continuity program. These plans and procedures should also be evaluated pre- and post-event, tested or exercised, and assessed during the development of corrective action plans. Objective evaluations and assessments, developed from tests and exercises, provide feedback on continuity planning, procedures, and training. This feedback in turn supports a corrective action process that helps to establish priorities, informs budget decision making, and drives improvements in plans and procedures. This continuity program management cycle, as illustrated in Figure 1, should be used by all organizations as they develop and implement their continuity programs.

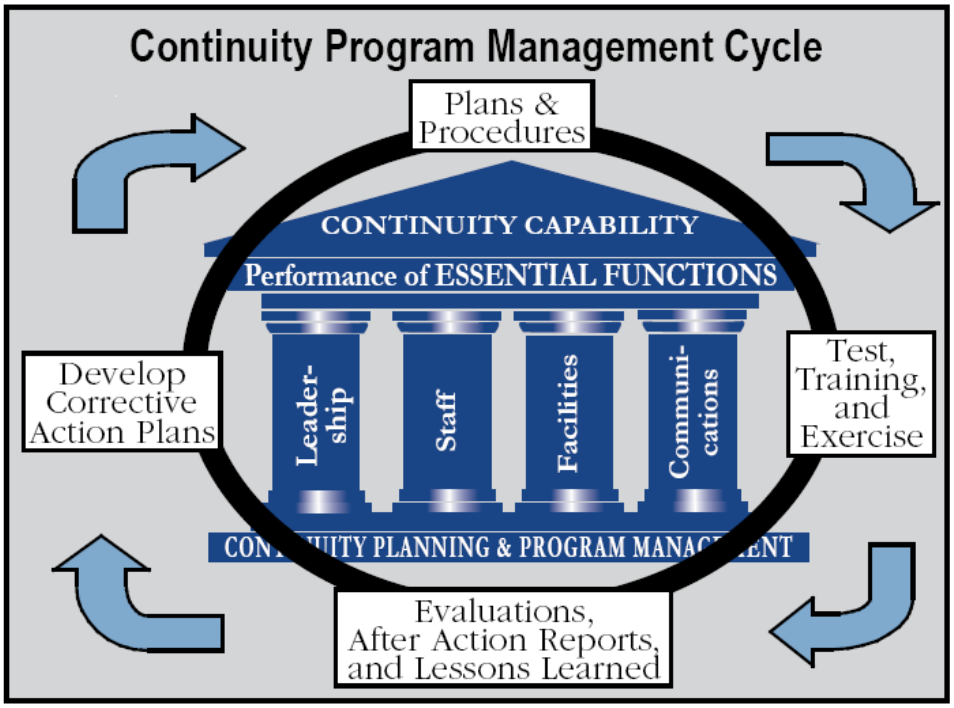


Figure 1

To support the continuity program management cycle, organizations should develop a continuity multi-year strategy and program management plan (MYSPMP) that provides for the development, maintenance, and annual review of continuity capabilities, requiring an agency to:

a. Designate and review MEFs and PMEFs, as applicable.
b. Define both short-term and long-term goals and objectives for plans and procedures.

c. Identify issues, concerns, and potential obstacles to implementing the program, as well as a strategy for addressing these, as appropriate.
d. Establish planning, training, and exercise activities, as well as milestones for accomplishing these activities.
e. Identify the people, infrastructure, communications, transportation, and other resources needed to support the program.
f. Forecast and establish budgetary requirements to support the program.
g. Apply risk management principles to ensure that appropriate operational readiness decisions are based on the probability of an attack or other incident and its consequences.
h. Incorporate geographic dispersion into the organization's normal daily operations, as appropriate.
i. Integrate the organization's security strategies that address personnel, physical, and information security to protect plans, personnel, facilities, and capabilities, to prevent adversaries from disrupting continuity plans and operations.
j. Each organization shall develop a Corrective Action Program (CAP) to assist in documenting, prioritizing, and resourcing continuity issues identified during TT&E, assessments, and emergency operations.

See Annex A – Program Plans and Procedures

Risk Management

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

See Annex B – Risk Management

Budgeting

Budgeting for and acquiring resources for continuity capabilities is one of the most important components of continuity planning. These budgetary requirements will directly support the ability of headquarters (HQ) organizations and subordinate components to meet all the criteria of a viable continuity capability as stated in this CGC.

See Annex C – Budgeting and Acquisition of Resources

9. ELEMENTS OF A VIABLE CONTINUITY CAPABILITY FOR NON-FEDERAL ENTITIES: NSPD-51/HSPD-20 outlines the overarching continuity requirements for all government agencies and private sector organizations. These requirements are discussed in more depth in the "Key Considerations and Concept of Operations" section of the National Continuity Policy Implementation Plan. These "key components" are further delineated into the following elements of continuity.

a. ESSENTIAL FUNCTIONS. The identification and prioritization of essential functions is a prerequisite for continuity planning, because they establish the planning parameters that drive an organization's efforts in all other planning and preparedness areas. Resources and staff will likely be limited during an event that disrupts or has the potential to disrupt normal activities and that necessitates the activation of continuity plans, preventing the organization from performing all of its normal functions or services. Therefore, a subset of those functions that are determined to be critical activities are defined as the organization's essential functions. These essential functions are then used to identify supporting tasks and resources that should be included in the organization's continuity planning process.

The National Continuity Policy Implementation Plan has established three categories of essential functions: NEFs, PMEFs, and MEFs. The ultimate goal of continuity in the Federal executive branch is the continuation of NEFs. To achieve that goal, the objective for non-federal entities is to identify their MEFs and PMEFs, as appropriate, and ensure that those functions can be continued throughout, or resumed rapidly after, a disruption of normal activities.

The eight **National Essential Functions (NEFs)** (listed in Annex D of this document) represent the overarching responsibilities of the Federal Government to lead and sustain the Nation and will be the primary focus of the Federal Government's leadership during and in the aftermath of an emergency.

Primary Mission Essential Functions (PMEFs) are Mission Essential Functions 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.

Mission Essential Functions (MEFs) are a broader set of essential functions that includes not only an organization's PMEFs, but also all other organization functions that must be continued throughout or resumed rapidly after a disruption of normal activities, but that do not rise to the level of being PMEFs. MEFs are those functions that enable an organization to provide vital services, exercise civil authority, maintain the safety of the public, and sustain the industrial/economic base during disruption of normal operations.

When identifying an organization's essential functions and categorizing them as MEFs or PMEFs, organizations with incident management responsibilities must incorporate these into their continuity planning requirements for performing these functions. Integration of continuity planning with incident management planning and operations include responsibilities delineated in the National Response Framework (NRF) and is linked to an organization's ability to conduct its essential functions.

See Annex D – Essential Functions

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

See Annex E – Orders of Succession

c. DELEGATIONS OF AUTHORITY. To ensure a rapid response to any emergency requiring the implementation of its continuity plan, an organization should delegate authorities for making policy determinations and other decisions, at the field, satellite, and other organizational levels, as appropriate. It is vital to clearly establish delegations of authority, so that all organization personnel know who has the right to make key decisions during a continuity situation. Generally, a predetermined delegation of authority will take effect when normal channels of direction and control are disrupted and will lapse when those channels are reestablished.

See Annex F – Delegations of Authority

d. CONTINUITY FACILITIES. As part of their continuity planning, all non-federal entities should identify continuity facilities; alternate uses for existing facilities; and, as appropriate, virtual office options including telework. Risk assessments should be conducted on these facilities to provide reliable and comprehensive data to inform risk mitigation decisions that will allow non-federal entities to protect assets, systems, networks, and functions while determining the likely causes and impacts of any disruption. All personnel should be briefed on organization continuity plans that involve using, or relocating personnel to continuity facilities, existing facilities, or virtual offices. Continuity personnel should be provided supplemental training and guidance on relocation procedures.

See Annex G – Continuity Facilities

e. CONTINUITY COMMUNICATIONS. The ability of an organization to execute its essential functions at its continuity facilities depends on the identification, availability, and redundancy of critical communications and information technology (IT) systems to support connectivity among key leadership personnel, internal organization elements, federal and other non-federal entities, critical customers, and the public, during crisis and disaster conditions. The capabilities of communications and IT systems (e.g., secure and non-secure voice systems, video conferencing, and fax and other messaging capabilities) to be used during an incident should mirror those capabilities used during day-to-day operations, and the choice of communications and IT systems should consider how resilient those systems are and how capable they are of operating under conditions that may involve power or other infrastructure disruptions. All necessary and required communications and IT capabilities

should be operational as soon as possible following the continuity activation, and in all cases within 12 hours of continuity activation. Organizations need to plan accordingly for essential functions that require uninterrupted communications and IT support.

See Annex H – Continuity Communications

f. VITAL RECORDS MANAGEMENT. Another critical element of a viable continuity plan and program includes the identification, protection, and availability of electronic and hardcopy documents, references, records, information systems, and data management software and equipment (including classified and other sensitive data) needed to support essential functions during a continuity situation. Personnel should have access to and be able to use these records and systems to perform essential functions and to reconstitute back to normal organization operations. Organizations should pre-position and regularly update duplicate Emergency Operating Records to ensure performance of essential functions.

See Annex I – Vital Records Management

g. HUMAN CAPITAL.

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

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

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

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

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

See Annex J – Human Capital

h. TEST, TRAINING, AND EXERCISE (TT&E) PROGRAM. An effective TT&E program is necessary to assist organizations to prepare and validate their organization's continuity capabilities and program to perform essential functions 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 organization essential functions.

Training provides the skills and familiarizes leadership and staff with the procedures and tasks they should perform in executing continuity plans. Tests and exercises serve to assess and validate all the components of continuity plans, policies, procedures, systems, and facilities used to respond to and recover from an emergency situation and identify issues for subsequent improvement. All organizations should 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 should be documented in an organization's CAP Improvement Plan (IP).

See Annex K – Test, Training, and Exercise

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

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

See Annex L – Devolution of Control and Direction

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

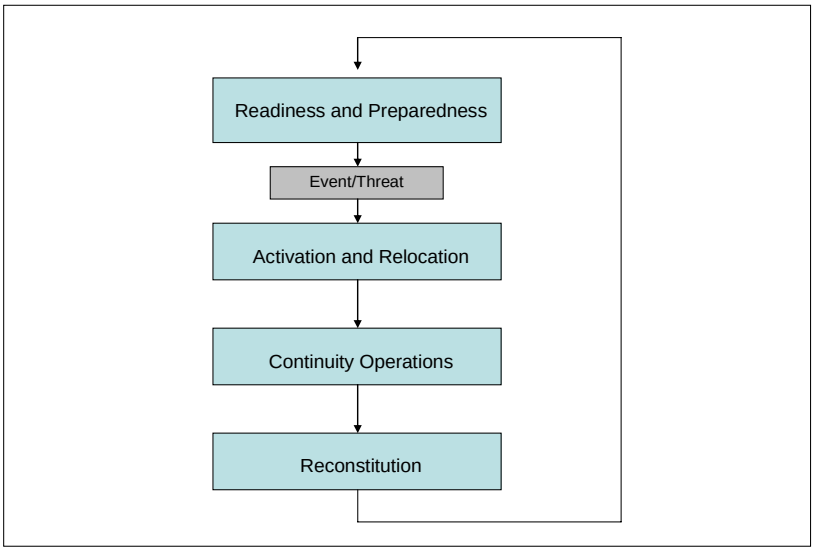
See Annex M – Reconstitution Operations

10. COORDINATION WITH NON-FEDERAL ENTITIES AND FEDERAL DEPARTMENTS AND AGENCIES: The Federal Government's NEFs, prescribed in NSPD-51/HSPD-20, cannot be performed without the robust involvement of non-federal entities. The Nation's non-federal entities play an integral role in determining the needs of the public and in ensuring that essential functions (e.g., police and fire services, emergency medical care, road construction, public education) continue on a daily basis. The Federal departments and agencies' continuity plans and operations shall be appropriately integrated with the emergency and continuity plans and capabilities of non-federal entities, as appropriate, in order to promote interoperability and prevent redundancies and conflicting lines of authority.

Non-federal entities should coordinate with Federal departments and agencies, as appropriate, to build relationships and ensure unity of effort by:

a. Incorporating their capabilities into the organization's continuity planning and exercise activities to the extent possible.
b. Identifying hazards relevant to the organization's mission and location.
c. Partnering with these entities to develop continuity plans that are coordinated with Federal plans, to the extent possible.
d. Participating in continuity working groups (CWGs), information sharing, training, and exercises, as appropriate.
e. Coordinating occupant emergency plans (OEPs), shelter-in-place (SIP) plans, and regional and local evacuation plans.
f. Participating in existing alert and notification networks and credentialing initiatives, as appropriate.
g. Identifying interdependencies and ensuring resiliency with critical infrastructure and services at all levels.
h. Coordinating continuity resource and security requirements, as appropriate.
i. Participating in other coordinating activities, as appropriate.

11. <u>CONTINUITY PLAN OPERATIONAL PHASES AND IMPLEMENTATION</u>: A continuity plan is implemented to ensure the continuation or rapid resumption of essential functions during a continuity event. Organizations should develop an executive decision-making process that allows for a review of the emergency situation and a determination of the best course of action based on the organization's readiness posture. An organization's continuity implementation process should include the following four phases: readiness and preparedness, activation and relocation, continuity operations, and reconstitution. The four phases are implemented as illustrated in Figure 2.



.

Figure 2

See Annex N – Continuity Plan Operational Phases and Implementation

12. <u>ROLES AND RESPONSIBILITIES:</u> The following responsibilities are assigned to the leadership of designated entities listed below. Non-federal entities play an integral role in determining and supporting 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). Non-federal entities should work with their tribal, local, State, and Federal partners and the private sector in developing and coordinating continuity plans. This coordination helps facilitate the resourcing and allocation of resources for the development of continuity plans and the procurement of emergency response equipment, as appropriate.

a. **Elected Officials:**

At all jurisdictional levels, Elected Officials are responsible for ensuring that continuity programs are appropriately resourced and that responsible and effective continuity leaders and managers are appointed or hired to direct those programs. Elected Officials should develop a Continuity Planning Team that encompasses all of the departments, divisions, or other offices within the organization. The Elected Officials should sign off on the final plans and policies developed by the Continuity Planning Team.

b. **Senior Leadership:**

Senior leadership is directly responsible for ensuring that continuity plans and programs are developed, coordinated, exercised, and capable of being implemented when required. Specific responsibilities include:

1) Designating a Continuity Manager and Coordinator, as appropriate, for their organization.
2) Approving all required continuity plans and programs.
3) Notifying appropriate offices and organizations upon execution of continuity plans.
4) Supporting the work of the Continuity Manager and Coordinator for their organization, including providing the necessary budgetary and other resources to support the continuity program, as required.

c. **Continuity Manager:**

The Continuity Manager will coordinate the overall activities of the Continuity Planning Team for the jurisdiction. The Continuity Manager will provide an annual summary of planning activities to the Elected Officials and department heads.

d. **Continuity Coordinator:**

Regardless of organizational or jurisdictional level, general responsibilities of the Continuity Coordinator include:

1) Coordinating continuity planning activities with policies, plans, and initiatives related to critical infrastructure protection.
2) Being in charge of creating and leading the continuity planning.
3) Directing and participating in periodic cross-jurisdictional continuity exercises.
4) Establishing a MYSPMP designed to achieve continuity objectives.
5) Coordinating the continuity input of the organization and ensuring those inputs reflect and support the intent of the overall continuity plan and the sustainment of essential functions.
6) Developing and maintaining the continuity plan.
7) Developing and administrating a continuity program budget and submitting funding requirements to the agency head.
8) Serving as an advocate for the continuity plan and program.

e. **Continuity Planning Team:**

The Continuity Planning Team coordinates continuity planning and duties for the entire organization. These duties include:

1) Overall continuity coordination for the organization.
2) Providing guidance and support for development of the organization’s continuity plan.

3) Establishing of a CWG for their organization or office, which serves as the principal continuity coordinating organization and forum for exchanging ideas and information regarding continuity planning, procedures and resources for that organization.
4) Coordinating continuity exercises, documenting post-exercise lessons learned, and conducting periodic evaluations of organizational continuity capabilities.
5) Understanding the role that adjacent jurisdictions and organizations might be expected to play in certain types of emergency conditions and what support those adjacent organizations might provide.
6) Understanding the limits of their continuity resources and support capabilities.
7) Anticipating the point at which adjacent organizational or mutual aid resources will be required.

f. **Individuals are responsible for:**

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

13. POINT OF CONTACT: Should you have any questions or need additional assistance with the information contained in the CGC 1, please contact the Assistant Administrator, FEMA National Continuity Programs (NCP) Directorate, at 202.646.4145.

14. DISTRIBUTION: CGC 1 is authorized to be distributed to all U.S. Non-Federal Entity organizations and other interested parties.

ANNEX A. PROGRAM PLANS AND PROCEDURES

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

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

1. Ensuring that an organization can perform its MEFs and PMEFs, if applicable, under all conditions.
2. Reducing the loss of life and minimizing property damage and loss.
3. Executing a successful order of succession with accompanying authorities in the event a disruption renders that organization's leadership unable, unavailable, or incapable of assuming and performing their authorities and responsibilities of office.
4. Reducing or mitigating disruptions to operations.
5. Ensuring that the organization has facilities where it can continue to perform its MEFs and PMEFs, as appropriate, during a continuity event.
6. Protecting essential facilities, equipment, records, and other assets, in the event of a disruption.
7. Achieving the organization's timely and orderly recovery and reconstitution from an emergency.
8. Ensuring and validating continuity readiness through a dynamic and integrated continuity TT&E program and operational capability.

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

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

- The consequences of not protecting valuable assets (e.g., people, information, and facilities) and/or not performing essential functions

- The threat environment (as it relates to a particular organization or area of concern)
- The level of vulnerability to the relevant threats

Reviewing an organization's risks and risk management programs should take into consideration additional factors such as the probabilities of events occurring, mission priorities, and impact assessments. Further, cost may also be a factor to consider, because informed decisions about acceptable and unacceptable levels of risk will ultimately drive the expenditure of resources (e.g., money, people, and time) to mitigate risk. Risk can never be fully mitigated, because no organization can afford to counter every threat to its mission. Successful continuity planning demands an intelligent analysis and prioritization of where and when to focus resources and the allocation of funding and other assets to support the continuity program.

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

As an integral part of risk management, an organization's leaders should think beyond the internal effects of their inability to perform essential functions and provide essential services. Organization heads and staff at all levels should also consider the interdependencies between and among organizations that share critical roles in the delivery of NEF capabilities.

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

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

appropriate, to ensure the performance of the organization's essential functions. Classification restrictions must be considered during this process.

7. Provide the ability to recover from the effects of an emergency and reconstitute operations and resources, so that the organization can return to a fully operational condition in the aftermath of an incident. Organizations should coordinate and plan as necessary, to ensure a return to normal operations.
8. Identify the components, processes, and requirements for the identification, training, and preparedness of personnel who are capable of relocating to continuity facilities to support the continuation of the performance of essential functions.
9. Identify the components, processes, and requirements that ensure the continued performance of an organization's essential functions.
10. Outline a process for determining the organization's readiness posture and for decision making regarding its corresponding actions to implement continuity plans and procedures.
11. Establish alert and notification procedures for all continuity personnel throughout all phases of a continuity event. Provide a process for reporting continuity readiness and activation status.
12. Define the roles and responsibilities of those individuals who support the organization's continuity program.
13. Establish and maintain appropriate point of contact (POC) rosters of trained continuity personnel who are fully equipped and who have the authority to perform essential functions, including the execution of the devolution of control plan.
14. Establish and maintain the appropriate relocation procedures and guidance for continuity personnel.
15. Provide the ability to communicate with and coordinate activities with non-continuity personnel.
16. Ensure that the continuity of operations plan can be implemented both with and without warning.
17. Ensure that the continuity of operations plan can become operational within the minimal acceptable period for MEF disruption.
18. Ensure that in all cases, PMEFs will be either performed continuously during the course of an event or resumed within 12 hours of an event.
19. Ensure that sustained operations can be maintained for up to 30 days after an event or until normal business activities can be resumed. This includes planning for the challenges posed by extended events (like a pandemic) that occur in repeated waves.
20. Ensure there is a provision for an all-hazards risk assessment of all organization continuity facilities.
21. Identification and preparation of all organization continuity facilities.
22. Recommended content and maintenance of drive-away kits.
23. Include consideration of all of the requirements and procedures needed to perform essential functions, including the establishment of contingency plans in the event that key resources are not available.

24. Include provisions and procedures for assisting all organization staff, especially those who are disaster victims, with special human capital concerns following a catastrophic disaster.
25. Provide guidance to all staff in developing Family Support Plans which will increase personal and family preparedness throughout the organization.

CONTINUITY CONSIDERATIONS AND METRICS: From the list of continuity considerations listed below, organization heads should use these key questions and metrics guidance to certify that their organizations have a robust continuity capability.

	Continuity Requirements	Key Questions	Metrics
1	The continuation of the performance of essential functions during any emergency should 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 essential functions 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 essential functions 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 should 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 should 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 to safeguard vital resources, facilities and records. ▪ Document measures taken to ensure official access to vital resources, facilities and records.
4	Provision should 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

	Continuity Requirements	Key Questions	Metrics
5	Provision should 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 should be made for reconstitution capabilities that allow for recovery from a catastrophic emergency and resumption of normal operations; and	▪ What is your plan for ensuring your reconstitution capability?	▪ Identify your reconstitution capability plan.
7	Provision should be made for the identification, training, and preparedness of personnel capable of relocating to continuity facilities to support the continuation of the performance of essential functions.	▪ Have you identified, trained, and prepared personnel to relocate to alternate sites to continue essential functions?	▪ Verify that staff are identified, trained, and prepared to relocate to alternate sites.

Table 1: Continuity Considerations and Metrics

For each of the seven continuity considerations, senior leadership should self-identify a simple grading system to show status such as:

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

Organizations may use FEMA's more detailed Continuity Evaluation Tool (CET) to measure their continuity readiness against the guidance contained in NSPD-51/HSPD-20, the National Continuity Policy Implementation Plan, Federal Continuity Directive 1 (FCD 1), and this Continuity Guidance for Non-Federal Entities.

PLANNING STRATEGY: The Planning Team should create an overall continuity strategy that is agreed upon by the Elected Officials or other organizational leadership prior to the development of the detailed continuity plan. This strategy will establish a policy-level framework to guide decisions made later during detailed planning for continuity implementation.

There are several approaches to developing a continuity strategy and each should be considered when developing continuity plans and programs. These may include the more traditional continuity planning where ERG staff perform designated essential functions from a continuity facility, a devolution option, where responsibilities are transferred to both alternate staff as well as continuity facilities, or even a telecommute/virtual office option where ERG or other staff perform essential functions from home or another remote location. The activation of a continuity

plan may also entail the immediate activation of cross-organizational support agreements regardless of the broad continuity strategy that is adopted.

PLANNING INTEGRATION: In order to ensure the resiliency and survivability of essential services, community governments and other organizations will need to work together to coordinate their continuity plans with those of neighboring jurisdictions (horizontal integration) and with Federal and non-federal entities to ensure local plans are well-coordinated with their functional counterparts at other levels of government (vertical integration). Continuity plans should also be coordinated with non-federal and federal preparedness, response, and Homeland Security related plans, and other plans as appropriate.

Example of Vertical and Horizontal Integration

One aspect of horizontal integration may be addressed in the mutual support/aid relationship a city police department has with other police departments in adjacent jurisdictions. Mutual support/aid agreements with adjacent jurisdictions may reflect the region-wide shared use of law enforcement facilities, equipment, and personnel. Vertical planning integration may be addressed in the pre-coordinated agreements between the city police department and the respective law enforcement agency at the next higher level of government and, once again, address mutual support, interoperability, and the shared use of law enforcement personnel, equipment and facilities (see Figure 3).

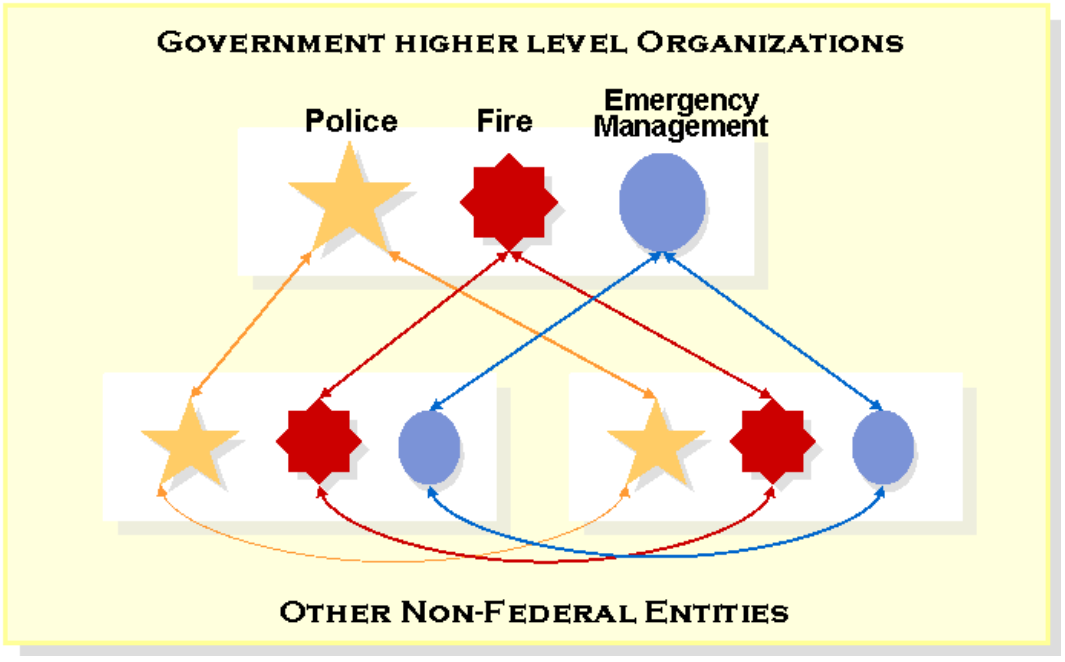


Figure 3

ANNEX B. RISK MANAGEMENT

Risk management is a process to identify, control, and minimize the impact of uncertain events. This process supports the overarching Continuity Program Management Cycle by identifying (1) the critical risks to organizational readiness and (2) the strategies that best mitigate the risks. The recommended risk management cycle is made up of five analytical and management phases (see Figure 4): (1) setting strategic goals and objectives, and determining constraints; (2) assessing the risks; (3) evaluating alternatives for addressing these risks; (4) selecting the appropriate alternatives; and (5) implementing the alternatives and monitoring the progress made and the results achieved. The risk management cycle provides a useful framework for maximizing the readiness of an organization to provide its primary mission essential functions in the face of risks from a broad spectrum of hazards facing the organization, both manmade and natural. This process organizes information about the possibility of a spectrum of unwanted outcomes into an inclusive, orderly structure that helps decision makers make more informed choices about risks to the organization's readiness across the four pillars that comprise the Nation's continuity capability: leadership, staff, facilities, and communications.

Figure 4

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

Phase 1 – Strategic Goals, Objectives, and Constraints

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

- **Understand and define the decision**. For this effort, the critical question is: How should I invest my limited resources across the four continuity pillars – leadership, staff, facilities and communications – to ensure that my organization satisfies its continuity considerations?
- **Determine who should be involved**. Input from key stakeholders is essential to a sound risk management process. The analysis team should identify and solicit input from stakeholders who should be involved in making the decision, and those who will be affected by actions resulting from the decision making process.
- **Identify the factors that will influence the decisions**. The decision to invest resources to meet continuity considerations is not based on one factor. They require decision makers to simultaneously weigh multiple factors, including costs, timelines, and risks.

Phase 2 – Risk Assessment

This phase involves following a structured process for understanding the problem facing an organization. Simply, this process provides this understanding by answering the following three

questions: (1) what can go wrong, (2) what is the likelihood that the undesired event might occur; and (3) what would be the impact should it occur? Critical steps in this phase include:

- **Inventory the essential functions provided by the organization**. The analysis team should leverage the functions identified during the Essential Function Identification and Analysis process (see Annex D).
- **Identify the hazards that can impact delivery of the essential functions.** This step includes exploring potential natural events, intentional man-made events, and non-intentional man-made events that could adversely affect the ability of the organization to perform its essential functions. Natural hazards are those where the occurrence is beyond the control of the organization, including earthquakes, floods, ice storms, winter weather, and external fires. Intentional man-made hazards are also beyond the direct control of the organization and could include events such as external sabotage, and terrorism. Non-intentional man-made events, such as power outages, fires, explosions, equipment failures, or human errors may be within the control of the organization.
- **Develop continuity hazard scenarios.** All of the assessment steps should be performed within the context of a set of scenarios, each of which is a unique combination of a particular hazard and the organization's essential functions. Within each scenario, the analysis team should consider risks to all four continuity pillars, as appropriate, recognizing that in most cases, all of the pillars should be available in order to deliver the function. The following steps outline the elements of the scenario risk assessment:

  - **Determine the risk information needed to assess the risk.** Describe the information necessary to assess the risk for each scenario. For each information item, specify the information type, precision, and certainty required, and the analysis resources available.
  - **Assess the risk**. For each scenario, the analysis team should assess the threat, vulnerability, and consequence, where:

    - Threat is the likelihood of a type of attack that might be attempted, or that the scenario will occur
    - Vulnerability is the likelihood that an attacker would succeed with a particular attack type, or that the scenario will result in the expected level of consequence
    - Consequence is the potential impact of a particular attack, or the negative impact of the scenario

    For this effort, consequence should be expressed in terms of failure to deliver the essential functions (see Annex D). When evaluating consequences, the analysis team should consider both short- and long-term impacts for disasters and accidents as well as intended and unintended effects from intentional attacks.

    Depending on the nature of the scenario, the analysis team can use different tools to assess the scenario's risk. For instance, the team may be able to leverage historical accident reporting databases to assess the risk of accident scenarios; while detailed stochastic models may be available for assessing the risk of natural hazard scenarios.

For scenarios where historical data or detailed modeling are scarce, subject matter expertise should be leveraged to produce the risk assessment.

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

Phase 3 – Alternative Evaluation

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

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

Phase 4 – Management Selection

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

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

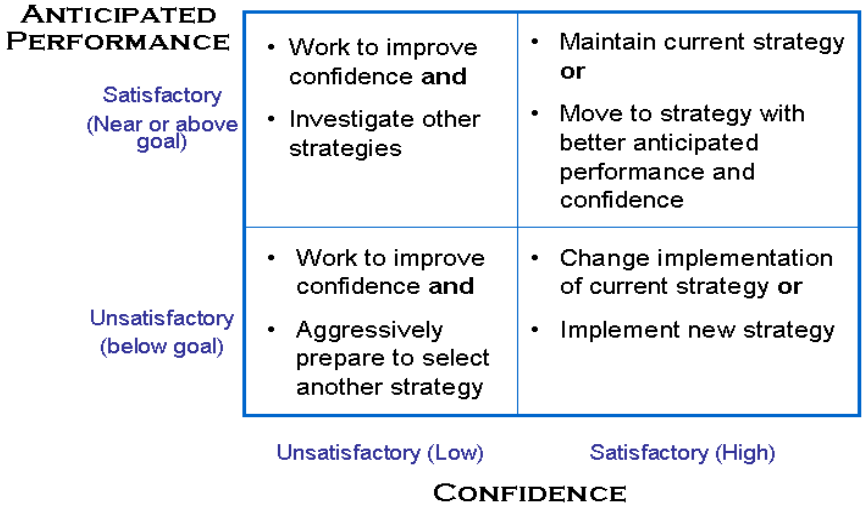


Figure 5

lower level.

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

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

Phase 5 – Implementation & Monitoring

Critical steps in this phase include:

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

Risk Management Support

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

ANNEX C. BUDGETING AND ACQUISITION OF RESOURCES

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

As recommended in NSPD-51/HSPD-20 and in the National Continuity Policy Implementation Plan, all organizations should identify and provide continuity funding and specific budgetary requirements for all levels of their organizations, including subordinate components and regional- and field-level offices. These budgetary procedures and requirements may directly support and enable organizations' ability to meet the criteria outlined in this Continuity Guide for a viable continuity of operations capability.

To ensure effective continuity capabilities, the organization should consider:

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

Budget and Acquisitions Considerations

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

1. Identifying the budgetary requirements for addressing continuity interdependencies in the performance of internal and other organizations essential functions.
2. Coordinating with the pre-established procurement mechanisms. Additional continuity factors such as probabilities of occurrence, mission priorities, and impact assessments, as part of the continuity risk management methodology.
3. Continuity budgets must also identify and plan for the funding and equipment to support continuity test, training, and exercise activities.

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

This page is intentionally left blank.

ANNEX D. ESSENTIAL FUNCTIONS

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

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

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

SECTION 1: MEFs

Organizations should provide a broad cross section of essential functions. The task of separating general operational functions from essential functions is an early and critical component of continuity planning. The process used to identify organizational functions may vary, depending on the mission and structure of an organization.

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

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

address all of them. In either case, the organization increases the risk that it will not be able to perform all of its essential functions during a continuity situation.

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

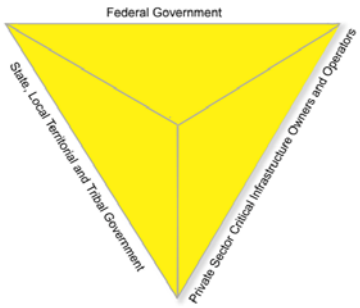


Figure 6

Continuity cannot occur without the commitment and dedication of many others who play integral roles in ensuring homeland security and provide essential functions and services to the Nation's citizens.
Those partners include the following (see Figure 6):

- Federal Government: legislative branch, executive branch (including all departments and agencies), and judicial branch;
- State, local, territorial, and tribal governments; and
- Private Sector Critical Infrastructure Owners and Operators.

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

- MEFs: The limited set of organization-level government functions that should be continued after a disruption of normal activities
- PMEFs: A subset of organization MEFs that directly support the NEFs
- NEFs: The eight functions the President and national leadership will focus on to lead and sustain the nation during a catastrophic emergency

The following relationship between government functions and mission essential functions is illustrated in Figures 7 and 8.

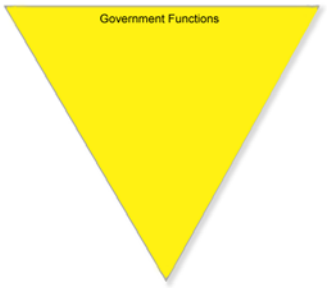


Figure 7

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

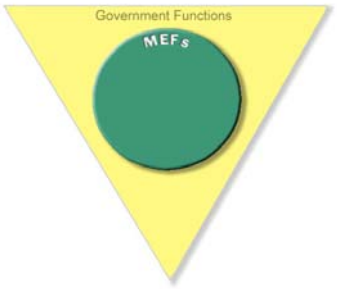


Figure 8

MEFs are described as the limited set of organization-level essential functions (as depicted in Figure 8) that should be continued throughout, or resumed rapidly after, a disruption of normal activities. MEFs are those functions that enable an organization to provide vital services, exercise civil authority, maintain the safety of the public, and sustain the industrial and economic base, during the disruption of normal operations. Once identified, MEFs serve as key continuity planning factors for organizations to determine appropriate staffing, communications, information, facilities, training, and other continuity requirements.

Process – MEF Identification and Analysis

Identifying all organizational MEFs is a prerequisite for continuity because it establishes the parameters that drive the organization's efforts in all other planning and preparedness areas. As an example a federal government function can be identified as a MEF, by utilizing the MEF Initial Screening Aid as referenced in the National Continuity Policy Implementation Plan (see Figure 9). Organizations can develop their own initial screening aid template, as appropriate.

MEF Initial Screening Aid		
Is the function directed by law, statute, presidential directive, or executive order? If yes, identify which:	**YES**	**NO**
Did a Business Process Analysis (BPA) determine that the function should 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.		

Figure 9

Organizations should do the following when identifying and analyzing MEFs:

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

SECTION 2: PMEFs

Once MEFs have been identified and analyzed, the planning process for identifying the PMEFs can begin. Directly linking PMEFs to a NEF requires organizations to identify the most essential functions that must continue during an emergency, as well as the planning required to perform those functions. This model identified in the National Continuity Policy Implementation Plan may serve as a template for non-federal entities.

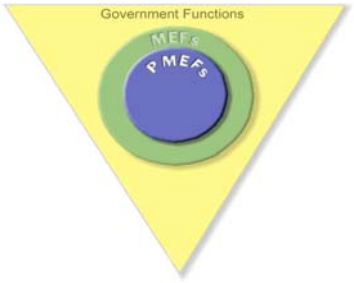


Figure 10

PMEFs are those department and agency mission essential functions, validated by the National Continuity Coordinator (NCC), which must be performed in order to support the performance of the NEFs before, during, and in the aftermath of an emergency (see Figure 10). 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.

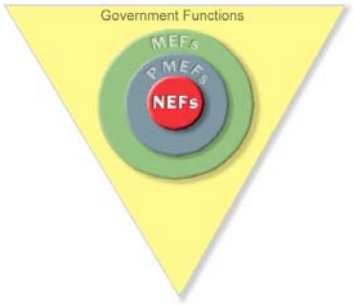


Figure 11

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 should be the primary focus of the Federal Government's leadership during and in the aftermath of an emergency (see Figure 11).

Figure 12 shows the interdependencies of the key partners and the functions of continuity. Federal government at all levels and non-federal entities are intimately connected and work together in critical partnership to ensure continuation of essential functions.

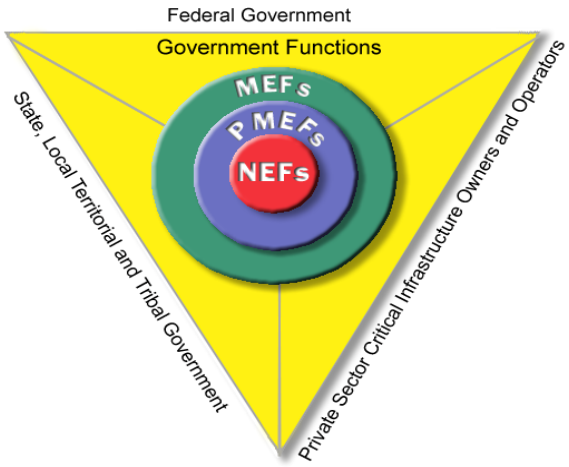


Figure 12

National Essential Functions (NEFs)

The eight NEFs are the foundation for all continuity programs and capabilities and represent the overarching responsibilities of the Federal government to lead and sustain the nation during a crisis, and therefore sustaining the following NEFs should be the primary focus of the Federal government leadership during and in the aftermath of an emergency that adversely affects the

performance of Government Functions. These are categories of functions performed by one or more agencies; they are not new authorities, requirements, or functions.

1. Ensuring the continued functioning of our form of government under the Constitution, including the functioning of the three separate branches of government. This NEF includes Federal executive branch functions that respect the roles and maintain the check and balance relationship among all three branches of the Federal government.
2. Provide leadership visible to the Nation and the world, and maintain the trust and confidence of the American people. This NEF includes organization 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 organization 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. Maintain and foster effective relationships with foreign nations. This NEF includes organization 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 organization 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. Provide rapid and effective responses to and recovery from the domestic consequences of an attack or other incident. This NEF includes organization functions to implement response and recovery plans including, but not limited to, the implementation of the NRF.
7. Protecting and stabilizing the Nation's economy and ensuring public confidence in its financial systems. This NEF includes Federal executive department and organization 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. Provide critical Federal government services that address the national health, safety, and welfare needs of the United States. This NEF includes organization functions that ensure that the critical Federal-level health, safety, and welfare services of the Nation are provided during an emergency.

Process – PMEF Identification and Analysis

For an organization function to be identified as a PMEF, the National Continuity Policy Implementation Plan provides the following guidance (see Figure 13).

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 should be "YES" for the function to be considered a PMEF.		

Figure 13

The immediacy of maintaining or recovering essential functions capability is driven by the results of the MEF and NEF BPAs and the NEF Business Impact Analysis (BIA). 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.

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

ANNEX E. ORDERS OF SUCCESSION

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

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

1. Establish an order of succession for leadership. There should be a designated official available to serve as acting head until that official is appointed by appropriate authority, replaced by the permanently appointed official, or otherwise relieved.
    a. Geographical dispersion to include, if applicable, regional, field, or satellite leadership in the line of succession, is encouraged and ensures roles and responsibilities can transfer in all contingencies.
    b. Where a suitable field structure exists, appropriate personnel located outside of the subject region should be considered in the order of succession.
2. Establish orders of succession for other key leadership positions, including administrators, key managers, and other key mission essential personnel or equivalent positions. Order of succession should also be established for devolution counterparts in these positions.
3. Describe orders of succession by positions or titles, rather than by the names of the individuals holding those offices. To ensure their legal sufficiency, coordinate the development of orders of succession with the general counsel or other comparable legal authority.
4. Establish the rules and procedures designated officials should follow when facing the issues of succession to office.
5. Include in the succession procedures the conditions under which succession will take place in accordance with applicable laws and procedures; the method of notification; and any temporal, geographical, or organizational limitations to the authorities granted by the orders of succession.
6. Include orders of succession in the vital records and ensure they are available at the continuity facilities or other continuity of operations locations in the event the continuity plan is activated.
7. Revise orders of succession, as necessary, and distribute the revisions promptly as changes occur.

8. Develop and provide duties and responsibilities briefing to the designated successors of leadership, explain their responsibilities as successors and on any provisions for their relocation. Designated successors should receive annual refresher briefings.

ANNEX F. DELEGATIONS OF AUTHORITY

To ensure a rapid response to any emergency and to minimize disruptions that require continuity implementation, organizations should pre-delegate the authority to make policy determinations and decisions, at leadership levels and locations, as deemed appropriate. Delegations of authority identify who is authorized to act on behalf of senior leadership or other officials for specified purposes and ensures that designated individuals have the legal authorities to carry out their duties. To the extent possible, these authorities should be identified by title or position, and not by the individual office holder's name. Generally, predetermined delegations of authority will take effect when normal channels of direction are disrupted and will terminate when these channels are reestablished. Delegations of authority is an essential part of a continuity plan and should reach to a sufficient depth and have sufficient breadth—at least three positions deep and geographically dispersed where feasible—to ensure essential functions continue during emergencies. To ensure legal sufficiency and clarity, delegations of authority should consist of the following characteristics:

1. Delegations of authority should document in advance (where designated) the legal authority for officials to make key policy decisions during a continuity situation.
2. To ensure MEFs and PMEFs are performed, delegations of authority must be planned and documented in advance of an incident and in accordance with applicable laws, including by:
    a. Delineating the limits of authority and accountability.
    b. Outlining explicitly in a statement, the authority (including any exceptions to that authority) of an official so designated, to exercise direction, and the authority of an official to re-delegate functions and activities, as appropriate.
    c. Defining the circumstances under which delegation of authorities would take effect and would be terminated.
3. Delegations of authority should ensure that senior leadership or other officials who might be expected to assume authorities in a continuity situation are properly informed and trained, as required, to carry out their emergency responsibilities. Training of the senior leadership or other officials should be conducted at least annually.
4. Delegations of authority should ensure the orderly (and predefined) transition of leadership to include key supporting positions during an emergency.
5. Delegations of authority should be included in vital records and available at continuity facilities or other continuity locations in the event the continuity plan is activated.

This page is intentionally left blank.

ANNEX G. CONTINUITY FACILITIES

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

Daily operating facilities should be evaluated for hardness in accordance with applicable standards, and should consider 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, continuity facilities should 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 continuity facilities such that daily activities can be replaced or augmented with those needed during an emergency (often referred to as dual-use facilities).

Limited geographical size may complicate continuity planning and render communities with a relatively smaller footprint more prone to disruptive events than larger jurisdictions. For such a community, even if the continuity plan provides for relocation facilities, the geographical size of the jurisdiction may limit its ability to achieve any meaningful geographic separation between primary and continuity facilities. In such an instance, events that disrupt operations at the primary facility may also impact operational capabilities at the continuity facility. Small jurisdictions may simply lack the physical space to be able to relocate essential functions to continuity facilities that are geographically removed from the threat, but still within their jurisdictional limits. These organizations may want to consider mutual aid or other joint use agreements with neighboring jurisdictions to help facilitate their continuity preparedness.

Planning Requirements

Continuity facilities should provide:

1. Sufficient space, equipment and other resources to sustain essential operations, as appropriate, and ERG and support staff.
2. The capability to perform essential operations as soon as possible after an emergency or other continuity event with minimal disruption of operations and in all cases within 12 hours after an event; the ability to maintain this capability for up to 30 days after an event or until normal business activities can be resumed; and the capability to perform these essential operations under all threat conditions including the possible use of weapons of mass destruction (WMD). Some essential functions cannot be interrupted and continuity facilities should include support for these continuous operations.
3. Reliable logistical support, services, and infrastructure systems.
4. Consideration for the health, safety, and security of employees who have been relocated to those sites.

5. Continuity communications, including the means for secure communications if appropriate, with all identified essential internal and external organizations, as well as with customers and the public.
6. Computer equipment, software, and other automated data processing equipment necessary.
7. Capabilities to access and use vital records necessary to facilitate the performance of critical business functions.

Continuity Facility Options

At a minimum, organizations should identify and maintain a continuity facility. A continuity facility may be classified as one of the following two types:

1. Hot Site: A continuity facility that already has in place the computer, telecommunications, and environmental infrastructure required to recover critical business functions or information systems.
2. Warm Site: A continuity facility that is equipped with some hardware, and communications interfaces, electrical and environmental conditioning which is capable of providing backup after additional provisioning, software or customization is performed.

In addition, organizations may consider implementing other or nontraditional continuity facility options including:

1. Existing space –
   a. Remote/offsite training facilities. These facilities may include a training facility located near the organization's normal operating facility, but far enough away to afford some geographical dispersion.
   b. Jurisdictional or field offices. A jurisdictional office or a field office that could be used as a continuity facility.
2. Virtual offices – To be effective, this option should provide access to vital records and databases to support the business functions and the robust communications necessary to sustain operation of business functions.
   a. Work at home/telework. Many organizations allow employees to work from home. This capability should be leveraged to allow some continuity personnel to fulfill their required business functions while at home or at other off-site location.
   b. Telecommuting facilities. These facilities can accommodate, on a prearranged basis, some continuity personnel, to allow them to fulfill their required duties at those locations.
   c. Mobile office. This capability includes the use of mobile fly-away kits that can include continuity of operations equipment such as laptop computers, cell phones, and satellite communications equipment, which can be readily transported to a remote location.
3. Memorandum of Agreement (MOA)/Memorandum of Understanding (MOU) for co-location with another entity – One organization may relocate to another organization's facilities. The organization that is relocating could occupy available space in the receiving organization's facility, training facilities, field offices, or other available space.

a. Space procured and maintained by another organization – Some organizations offer space procurement services that could be used by organizations to support the need for continuity facilities.

b. Participation in a joint-use continuity facility – With this option, organizations should ensure that shared facilities are not overcommitted during a continuity situation. Several organizations may pool their resources to acquire space they can use jointly as a continuity facility. An organization may co-locate with another organization at a continuity-facility, but each organization should have individually designated space and other resources at that location to meet its own needs (i.e., support its business functions).

c. Alternate use of existing facilities – In certain types of continuity situations (e.g., a pandemic), a combination of facilities may be used to support continuity operations (e.g., social distancing).

Planning Considerations

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

1. Location of Facilities. Organizations should conduct an all-hazards risk assessment for all continuity of operations facilities. The assessment should include identification of all hazards that may affect the facility; a vulnerability assessment that determines the affects of all hazards on the facility; a cost-benefit analysis of implementing risk mitigation, prevention, or control measures; and a formal analysis by management of acceptable risk. Continuity facilities should be located in an area where the potential disruption of the organization's ability to initiate and sustain operations is minimized. When identifying and preparing continuity facilities, maximum use should be made of existing local or field infrastructures, including consideration for other supporting options such as telecommuting locations, work-at-home/telework agreements, virtual offices, and joint or shared facilities. Additionally, continuity facilities:

   a. Should be operational as soon as possible upon continuity activation with minimal disruption of operations, but recommended within 12 hours after activation of a continuity of operations plan, and be capable of sustaining operations for up to 30 days after an incident or until normal business operations can be resumed. Organizations should identify essential business functions that can not be disrupted for any period of time and continued under all conditions. These functions should be identified in their continuity plans, and organizations should plan to provide support for those essential business functions from their continuity facilities.

   b. Should have sufficient distance between the facility location or threatened area and other facilities (hazardous materials sites, nuclear power plants) or locations (areas subject to natural disasters such as hurricanes and earthquakes) that are potential sources of disruptions or threats.

   c. Should have access to essential support resources such as food, water, fuel, medical facilities, and municipal services (e.g., fire, police).

d. Accessibility should include a defined transportation support plan that describes procedures for events with both warning and no warning.

e. Should be selected in locations that provide the alternate sites with power, telecommunication services, and Internet access, separate from those grids that provide their services to the primary facility, whenever possible.

2. Construction. Facilities should be selected and constructed so that they are not uniquely susceptible to risks associated with such natural disasters as earthquakes, tornadoes, hurricanes, or floods. Continuity facilities should have emergency/back-up power capability, so that essential business functions and operations can continue in the event the primary source of power is disrupted.

3. MOA/MOU. If the continuity facility is neither owned nor leased by the organization, a signed MOA/MOU should be prepared with the owner or occupant of the facility. This MOA/MOU should be reviewed annually. It is recommended that organizations coordinate with the appropriate organization for assistance in identifying relocation sites. MOAs/MOUs should specify:

   a. The required activation time between notifying the owner/occupant of the requirement to use the facility and the facility being available for occupancy by the organization as an alternate.

   b. Space and services to be provided at the facility.

   c. Sole use of allocated space by the organization during the period of occupancy.

4. Space. An organization's continuity facility space requirements should be sufficient to support all of the organization's continuity of operations staffing requirements. Contiguous space is desirable; however, noncontiguous space may be acceptable if there is adequate communications between emergency staff.

5. Preparation. After selecting appropriate sites, pre-positioning of critical resources, coordination with the site facility managers and agreements between the organization and property owners are necessary to ensure the continued availability of facility space and services. Organizations should have pre-positioned or have detailed site preparation and activation plans in order to achieve full operational capability within 12 hours of notification.

6. Billeting. Continuity plans should address housing to support continuity personnel at or near the continuity-facility site (e.g., billeting within facility, other locations, including motels or at emergency staffs home if it is within commuting distance to the alternate site).

7. Site Transportation. Transportation resource requirements, including transportation to/from the site and on a site should be included, as applicable.

8. Communications. The capability to communicate is critical to daily operations and absolutely essential in a crisis. The communications resources at the continuity facility should be sufficient to enable performance of all essential business functions. This includes providing sufficient quantity and mode/media to allow for effective interaction

with other organization elements. Secure and non-secure communications requirements should be incorporated.

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

The Acquisition Process

The process of acquiring a continuity facility includes: (1) identifying continuity-facility requirements, (2) selecting and acquiring the continuity facilities, and (3) reevaluating continuity facilities. These steps should be performed in consultation with the appropriate organization whenever possible.

Once selected, a continuity facility should be periodically reevaluated for their suitability and functionality. This should be done at least annually and whenever the organization's continuity of operations plan is reviewed and updated, to ensure that the facilities meet the continuity requirements.

This page is intentionally left blank.

ANNEX H. CONTINUITY COMMUNICATIONS

The success of continuity programs is dependent on the availability of robust and effective communications to provide internal and external connectivity. An organization's ability to execute its essential business functions at its primary facility and at its alternate or other continuity facilities, as well as the ability of the organization's senior leadership to collaborate, develop policy and recommendations, and act under all-hazards conditions, depend upon the availability of effective communications systems. These systems should support full connectivity, under all conditions, among key leadership, internal elements, other organizations, critical customers, and the public.

In accordance with the applicable laws and guidance, and other established communications requirements, an organization should:

1. Implement minimum communications requirements for its primary facilities and its alternate and other continuity facilities, as appropriate, which support the continuation of that organization's essential business functions.
2. Possess interoperable and available communications capabilities in sufficient quantity and mode/media, and that are commensurate with that organization's responsibilities during conditions of an emergency.
3. Possess communications capabilities that can support the organization's senior leadership while they are in transit to continuity facilities.
4. Ensure that the communications capabilities are maintained and readily available for a period of sustained usage of no less than 30 days or until normal operations can be reestablished, and that all continuity staff are properly trained, as appropriate, in the use of these communications capabilities.
5. Ensure the ability to provide assured and priority access to communications resources.
6. Have sufficient communications capabilities to accomplish that organization's essential business functions from an alternate or other continuity facility shared with another organization, and also have a signed agreement between those organizations, which ensures that each one has adequate access to communications resources.

(A recommended guidance or reference tool is the National Communications System's Directive 3-10.)

Organizations should possess, operate, and maintain, or have dedicated access to, communications capabilities at both their primary facility and continuity-facility locations, as well as mobile communications capabilities, to ensure the continuation of those organizations' functions across the full spectrum of hazards, threats, and emergencies, including catastrophic attacks or disasters.

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

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

This page is intentionally left blank.

ANNEX I. VITAL RECORDS MANAGEMENT

The identification, protection, and ready availability of vital records, databases, and hardcopy documents are critical elements of a successful continuity plan and program. In this document, "vital records" refers to information systems and applications, electronic and hardcopy documents, references, and records needed to support essential functions during a continuity situation.

Categories of vital records include the following:

Emergency Operating Records. These include records and databases essential to the continued functioning or the reconstitution of an organization during and after a continuity event. Examples of these records are emergency plans and directives, orders of succession, delegations of authority, staffing assignments, and related policy or procedural records. These records provide an organization's continuity personnel with the guidance they need to conduct operations during a continuity situation and to resume normal operations at the conclusion of that situation. Organizations should identify and preposition Emergency Operating Records needed to continue essential functions.

Rights and Interests Records. These include records critical to carrying out an organization's essential legal and financial functions, and vital to the protection of the legal and financial rights of individuals who are directly affected by that organization's activities. These records include those with such value that their loss would significantly impair the execution of essential organization functions, to the detriment of the legal or financial rights and entitlements of the organization and the affected individual(s). Examples of these records are accounts receivable files; contracting and acquisition files; official personnel records; Social Security, payroll, retirement, and insurance records; and property management and inventory records. Any Rights and Interests Records considered critical for continued performance of essential functions should be include in the Emergency Operating Records and maintained at the appropriate continuity facility.

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

1. An official vital records program:
    a. Identifies and protects those records that specify how an organization will operate in an emergency or disaster.
    b. Identifies those records necessary to the organization's continuing operations.
    c. Identifies those records needed to protect the legal and financial rights of the organization and citizens.

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

9. A vital records plan packet should be developed and maintained. The packet should include:
   a. A hard copy or electronic list of key organization personnel and disaster staff with up-to-date telephone numbers.
   b. A vital records inventory with the precise locations of vital records.
   c. Updates to the vital records.
   d. Necessary keys or access codes.
   e. Continuity-facility locations.
   f. Access requirements and lists of sources of equipment necessary to access the records (this may include hardware and software, microfilm readers, Internet access, and/or dedicated telephone lines).
   g. Lists of records-recovery experts and vendors.
   h. A copy of the organization's continuity of operations plan.

   This packet should be annually reviewed with the date and names of the personnel conducting the review documented in writing to ensure that the information is current. A copy should be securely maintained at the organization's continuity facilities and other locations where it is easily accessible to appropriate personnel when needed.
10. The development of an annual training program for all staff should include periodic briefings to managers about the vital records program and its relationship to their vital records and business needs. Staff training should focus on identifying, inventorying, protecting, storing, accessing, and updating the vital records.
11. There should be an annual review of the vital records program to address new security issues, identify problem areas, update information, and incorporate any additional vital records generated by new organization programs or functions or by organizational changes to existing programs or functions. The review will provide an opportunity to familiarize staff with all aspects of the vital records program. It is appropriate to conduct a review of the vital records program in conjunction with continuity exercises.
12. There should be annual testing of the capabilities for protecting classified and unclassified vital records and for providing access to them from the continuity facility.

Table 2 provides a useful way to assist organizations in identifying and managing their vital records.

Vital Records	Form of Record (e.g., hardcopy, electronic)	Pre-Positioned at Continuity Facility	Hand Carried to Continuity Facility	Storage Location(s)	Maintenance Frequency
		☐	☐		
		☐	☐		
		☐	☐		

Table 2: Identification of Vital Records

This page is intentionally left blank.

ANNEX J. HUMAN CAPITAL

In a continuity event, emergency employees and other special categories of employees will be activated by an organization to perform their assigned response duties. This set of employees includes continuity personnel, who will be referred to as members of the ERG. In addition to supporting the human capital needs of the organization's continuity personnel, agencies are responsible for managing their other human capital resources—those employees who have not been designated as continuity or ERG personnel but who will nevertheless be potentially affected by a continuity event. Organization plans and procedures for these employees should be addressed in the continuity of operations plan as well as in other types of emergency response planning documents, such as the organization's OEP or SIP plans.

Because of the need for organizations to be prepared for all-hazards emergencies and disasters, an organization should ensure that its human capital strategies for its continuity staff are adaptable to changing circumstances and a variety of emergencies, and that these strategies and procedures are regularly reviewed and updated as appropriate, as part of the organization's CAP.

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

Continuity Leadership and Staff

This section addresses those employees (e.g., ERG personnel) that perform the organization's essential functions during a continuity event. The following activities are associated with planning and preparedness for continuity of operations personnel:

1. **Organizations should develop and implement a process to identify, document, communicate with and train continuity personnel.** The identification of an organization's continuity personnel is a critical part of ensuring that an organization can successfully respond to a continuity event. Specific factors an organization should consider in developing and implementing this process include identifying:

    a. Personnel who perform essential functions as determined through the Business Process Analysis (BPA) (discussed in Annex D).
    b. Personnel who perform the supporting tasks that enable the performance of essential functions.
    c. Skill sets necessary to perform specific essential functions or to support tasks that enable the performance of those essential functions.

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

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

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

In addition to their continuity planning requirements, continuity personnel should understand their roles and responsibilities and participate in their organization's continuity TT&E program.

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

All Staff

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

3. **Organizations should implement a process to communicate the organization's operating status with all staff.** Organizations should follow the dismissal or closure procedures established for the facility or geographic region affected by an emergency situation that prevents significant numbers of employees from reporting for work on time or which require agencies to close all or part of their activities.

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

Human Capital Considerations

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

5. **Organizations should identify a human capital liaison—a continuity coordinator or a continuity manager—to work with the organization's human resources and emergency planning staff when developing the organization's emergency plans.** An organization's continuity coordinator should work closely with the organization's Chief Human Capital Officer or Director of Human Resources to resolve human capital issues related to a continuity event. The Chief Human Capital Officer or Director of Human Resources will ensure that the organization's policies remain current and relevant to changing environments or evolving threats. An organization's continuity programs, plans, or procedures should include organization-specific guidance and direction for continuity personnel on a wide range of human capital areas.

6. **Organizations should implement a process to communicate their human capital guidance for emergencies (pay, leave, staffing and other human resources flexibilities) to managers and make staff aware of that guidance in an effort to help agencies continue essential functions during an emergency.** Working with the Chief Human Capital Officer or Director of Human Resources, agencies should institute a process to communicate their human capital guidance for emergencies to managers, such as guidance on pay, leave, work scheduling, benefits, telework, hiring, etc., authorities and flexibilities. Pay, leave, staffing, and other human resources flexibilities available to agencies during an emergency are available through the organizations' human capital or human resources offices. In addition to communicating their human capital guidance to managers, organizations should institute methods for staff to become aware and familiar with the human capital guidance during emergencies such as utilizing an intranet website or employee orientation briefing.

Organization continuity coordinators should consult with their Chief Human Capital Officer or Director of Human Resources on ways to meet the six requirements of human capital planning for continuity identified above.

This page is intentionally left blank.

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

An effective TT&E program is necessary to assist organizations to prepare and validate their organization's capabilities and program and ability to perform essential functions 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 organization essential functions.

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

Testing

Testing ensures that equipment and procedures are maintained in a constant state of readiness to support continuity activation and operations. An organization's test program should include:

1. Annual testing (at a minimum) of alert, notification, and activation procedures for continuity personnel, with recommended quarterly testing of such procedures for continuity personnel.
2. Annual testing of plans for recovering vital records (both classified and unclassified), critical information systems, services, and data.
3. Annual testing of primary and backup infrastructure systems and services (e.g., for power, water, fuel) at continuity facilities.
4. Annual testing and exercising of required physical security capabilities.
5. Testing and validating equipment to ensure the internal and external interoperability and viability of communications systems, through quarterly testing of the continuity communications capabilities outlined in Annex H (e.g., secure and non-secure voice and data communications).
6. Annual testing of the capabilities required to perform an organization's essential functions, as identified in the BPA.
7. A process for formally documenting and reporting tests and their results.
8. Conducting annual testing of internal and external interdependencies identified in the organization's continuity plan, with respect to performance of an organization's and other organization's essential functions.

Training

Training familiarizes continuity personnel with their procedures, tasks, roles, and responsibilities in executing an organization's essential functions in a continuity environment. An organization's training program should include:

1. Annual continuity awareness briefings (or other means of orientation) for the entire workforce.
2. Annual training for personnel (including host or contractor personnel) who are assigned to activate, support, and sustain continuity operations.
3. Annual training for the organization's leadership on that organization's essential functions, including training on individual position responsibilities.
4. Annual training for all organization personnel who assume the authority and responsibility of the organization's leadership if that leadership is incapacitated or becomes otherwise unavailable during a continuity situation.
5. Annual training for all pre-delegated authorities for making policy determinations and other decisions, at the field, satellite, and other organizational levels, as appropriate.
6. Personnel briefings on organization continuity plans that involve using, or relocating to continuity facilities, existing facilities, or virtual offices.
7. Annual training on the capabilities of communications and IT systems to be used during an incident.
8. Annual training regarding identification, protection, and ready availability of electronic and hardcopy documents, references, records, information systems, and data management software and equipment (including sensitive data) needed to support essential functions during a continuity situation.
9. Annual training on an organization's devolution option for continuity, to address how each organization will identify and conduct its essential functions during an increased threat situation or in the aftermath of a catastrophic emergency.
10. Annual training for all reconstitution plans and procedures to resume normal organization operations from the original or replacement primary operating facility.

Training should prepare continuity personnel to respond to all emergencies and disasters and ensure performance of the organization's essential functions. These include interdependencies both within and external to the organization. As part of its training program, the organization should document the training conducted, the date of training, those completing the training, and by whom.

Exercises

An organization's continuity exercise program focuses primarily on evaluating capabilities or an element of a capability, such as a plan or policy, in a simulated situation. Organizations should refer to the Homeland Security Exercise and Evaluation Program (HSEEP) for additional exercise and evaluation guidance.

An organization's exercise program should include:

1. An annual opportunity for continuity personnel to demonstrate their familiarity with continuity plans and procedures and to demonstrate the organization's capability to continue its essential functions.
2. An annual exercise that incorporates the deliberate and preplanned movement of continuity personnel to an alternative facility or other continuity location.
3. Communications capabilities and both inter- and intra-organization dependencies.
4. An opportunity to demonstrate that backup data and records required to support essential functions at continuity facilities or locations are sufficient, complete, and current.
5. An opportunity for continuity personnel to demonstrate their familiarity with the reconstitution procedures to transition from a continuity environment to normal activities when appropriate.
6. An opportunity for continuity personnel to demonstrate their familiarity with the devolution procedures to reconstitute from a continuity environment to normal activities when appropriate.
7. A comprehensive debriefing after each exercise, which allows participants to identify systemic weakness in plans and procedures and to recommend revisions to the organization's continuity plan.
8. A cycle of events that incorporates evaluations, AARs, and lessons learned into the development and implementation of a Corrective Action Program (CAP), to include an Improvement Plan (IP).
9. Organizational participation: conducting and documenting annual assessments of their continuity TT&E programs and continuity plans and programs.
10. Each organization should 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:

    a. Identify continuity deficiencies and other areas requiring improvement and provide responsibilities and a timeline for corrective action;
    b. Identify program and other continuity funding requirements for submission to the organization leadership;
    c. Identify and incorporate efficient acquisition processes, and where appropriate, collect all inter-organization requirements into one action; and
    d. Identify continuity personnel requirements for an organization's leadership and their supporting Human Resource Offices.

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

The NEP does not preclude or replace exercise programs conducted by individual organizations, but it allows and encourages organizations to align their exercise programs to United States government-wide priorities. This may result in internal exercises that serve as building blocks

toward an organization's participation in NEP events, or it may result in proposals for incorporating an individual organization's continuity exercises within a NEP event. The HSEEP is a capabilities- and performance-based exercise plan that provides a standardized policy, methodology, and language for designing, developing, conducting, and evaluating all exercises. The HSEEP is a pillar of the NEP framework.

State, local, territorial and tribal government jurisdictions and private sector organizations should develop and maintain a continuity TT&E program for conducting and documenting TT&E activities.

Continuity Training Courses

The Federal Emergency Management Agency's Emergency Management Institute (EMI) and the University of Maryland offer several Continuity courses both on campus and through the Independent study series that is free and available to the non-federal community. All Independent Study (IS) courses may be found at http://training.fema.gov/is and by selecting the ISP Course List. EMI offers the following Continuity Independent Study and resident courses listed below:

- Continuity of Operations (COOP) Awareness Course (IS 546) 1 Hour.
- Introduction to Continuity of Operations (COOP) (IS 547) 5 Hours.
- Continuity of Operations (COOP) Program Managers Train-the-Trainer (TTT) (B/E/L 548) 3 Days.
- Continuity of Operations (COOP) Planning (TTT) (B/E/L 550) 3 Days.
- Devolution Planning Workshop (TTT) (B/E/L) 2 Days.
- Building Design for Homeland Security Continuity of Operations (COOP) (TTT) (B/E/L 156) 3 Days.

Emergency Management Institute Course Codes are defined as follows:

B Resident courses held at FEMA's Domestic Preparedness Noble Training Center.
E Resident courses held at the National Emergency Noble Training Center campus.
IS Independent Study courses.
L Resident courses held off-site.
TTT Train-the-Trainer.

IS 546 Continuity of Operations (COOP) Awareness Course

This one-hour web-based Continuity of Operations (COOP) Awareness course is designed for all public sector employees. The course provides a fundamental understanding of COOP, terms, objectives, and benefits to public sector organizations. It gives a brief overview of the elements of a viable COOP capability. This awareness course provides information on how a COOP event might affect employees, the organization and an employee's family. Both employees designated to be part of the Emergency Relocation Group (ERG) and those who are not will benefit from this course. The first lesson defines COOP, covers the basic concepts and benefits of COOP. Subsequent lessons explain the objectives of COOP planning and describe the basic elements of a viable COOP capability.

IS 547 Introduction to Continuity of Operations (COOP)

This five-hour web-based course is designed for a broad audience – from senior managers to those involved directly in the continuity of operations (COOP) planning effort. The course provides a working knowledge of the COOP guidance found in Federal Continuity Directive 1 (FCD 1), *Federal Executive Branch National Continuity Programs and Requirements*. The course provides activities to enhance your COOP program.

Topics covered in the course include an overview of what COOP is and the elements of a viable COOP program, as listed below.

- Essential Functions.
- Orders of Succession.
- Delegations of Authority.
- Continuity Facilities.
- Continuity Communications.
- Vital Records Management.
- Human Capital.
- Test, Training, and Exercise Program.
- Devolution of Control and Direction.
- Reconstitution Operations.

B/E/L 548 Continuity of Operations (COOP) Program Managers Train-the-Trainer (TTT)

This three-day course is designed to acquaint experienced COOP practitioners and instructors with the Continuity of Operations (COOP) Managers course materials. The objectives include defining COOP, explaining the benefits of a viable COOP program and plan, identifying elements of a viable COOP program, identifying processes, resources, and tasks necessary to implement and manage a successful COOP program. This training includes a "Train-the-Trainer" module to equip the managers to train the course to others.

B/E/L 550 Continuity of Operations (COOP) Planning Train-the-Trainer (TTT)

This three-day course is designed to assist continuity planners to develop Continuity of Operations (COOP) plans and programs. COOP plans facilitate the performance of essential functions during any situation which may disrupt normal operations. This training includes a "Train-the-Trainer" module to equip the managers to train the course to others.

B/E/L 551 Devolution Planning Workshop Train-the-Trainer (TTT)

This two-day course is designed to provide continuity planners with the tools and hands-on experience necessary to develop their organization's devolution plan. The objectives include identifying conditions under which devolution is appropriate, describing triggers for devolution, and identifying special considerations for devolution planning. This training includes a "Train-the-Trainer" module to equip the managers to train the course to others.

B/E/L 156 Building Design for Homeland Security for Continuity of Operations (COOP) Train-the-Trainer (TTT)

An important component of an effective continuity of operations plan and program is a facilities hazard analysis and vulnerability assessment. This risk assessment is critical because it helps senior leaders and continuity of operations program managers identify linkages to and weaknesses in buildings and other infrastructures that their organizations use when providing essential functions and services.

To support this requirement, NCP Continuity of Operations Division, in conjunction with FEMA's Mitigation Division, fielded the Building Design for Homeland Security Train-the-Trainer Course (B/E/L 156). This course was redesigned in 2005 to specifically address continuity of operations preparedness requirements. Updated in 2008, the course outlines the purpose, requirements, and components of a risk assessment for continuity of operations continuity facilities and demonstrates how to use the electronic continuity of operations Alternate Site Assessment Tool. This training includes a "Train-the-Trainer" module to equip the managers to train the course to others.

The University of Maryland provides education under a federal grant for non-federal continuity personnel. To reserve your space in the resident courses, a FEMA Form 75-5 (General Admission Application) should be submitted through your State emergency management office. The University of Maryland courses may be found at http://www.umaryland.edu/dhscoop. The following is a list and description of available training courses that could help personnel develop skills in continuity planning:

- Preparing the States: Implementing Continuity of Operations Planning (MGT-331) 2 Days
- Preparing the States: Implementing Continuity of Operations Planning Train-the-Trainer (MGT-331-1) Half Day

MGT-331/MGT-331-1 Preparing the States: Implementing Continuity of Operations Planning

The course is designed for state, local and tribal emergency planners, or other personnel involved in COOP planning. A COOP plan enables governments and jurisdictions to preserve, maintain and/or reconstitute their capability to perform their essential functions in the event of any disaster or emergency that could potentially disrupt government/jurisdiction/private-sector operations and service.

This course is two days (MGT 331) with an optional half day Train-the-Trainer course (MGT 331-1). It is designed to equip participants with the tools necessary to develop and maintain successful COOP plans and to train other personnel in COOP planning that conforms to Federal Emergency Management Agency (FEMA) guidelines under new Federal Guidance, Federal Continuity Directives 1 and 2. The course goals are derived from the Nationwide Plan Review, the National Preparedness Goal, and the Target Capabilities List.

ANNEX L. DEVOLUTION OF CONTROL AND DIRECTION

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

At a minimum a devolution plan should:

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

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

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

This page is intentionally left blank.

ANNEX M. RECONSTITUTION OPERATIONS

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

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

Implementation actions associated with reconstitution include:

1. Informing all personnel that the actual emergency, or the threat of an emergency, no longer exists, and instructing personnel on how to resume normal operations.
2. Supervising either an orderly return to the normal operating facility or a move to another temporary facility or to a new permanent operating facility.
3. Verifying that all systems, communications, and other required capabilities are available and operational and that the organization is fully capable of accomplishing all essential functions and operations at the new or restored facility.
4. Conducting an after-action review of the effectiveness of the continuity of operations plans and procedures, identifying areas for improvement from the review, documenting these in the organization's CAP and then developing a remedial action plan as soon as possible after the reconstitution.
5. Identifying which (if any) records were affected by the incident, and working with the records office (or similar function in the organization) to ensure an effective transition or recovery of vital records and databases and other records that had not been designated as vital records, as part of the overall reconstitution effort.

This page is intentionally left blank.

ANNEX N. CONTINUITY PLAN OPERATIONAL PHASES AND IMPLEMENTATION

An organization should be prepared to implement executive decisions that are based upon a review of the emergency, and that then determine the best course of action based on the organization's readiness posture. The organization should develop an implementation plan that includes that organization's continuity of operations implementation criteria. The plan should cover the four phases of (1) readiness and preparedness, (2) activation and relocation, (3) continuity operations, and (4) reconstitution.

Readiness and Preparedness

Readiness is the ability of an organization to respond to a continuity incident or event. Although readiness is a function of planning and training, it is ultimately the responsibility of an organization's leadership to ensure that an organization—through normal procedures or with a continuity plan—can perform its mission essential functions before, during, and after all-hazards emergencies or disasters.

The implementation of a continuity plan and its associated procedures may require the use of primary and/or alternate or other facilities, depending upon the emergency and its affect on normal operations. Examples of scenarios that may require continuity of operations activation include, but are not limited to, the following:

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

Activation and Relocation (0-12 Hours)

The organization should provide a process or methodology for attaining operational capability at the continuity of operations site(s) as soon as possible and with minimal disruption to operations, but in all cases within 12 hours of activation. Organizations should also identify those essential functions that should be continued without disruption and ensure these can be conducted, under all conditions. The process should include the activation of plans, procedures, and schedules for

the continuation of essential functions, as well as for the personnel, vital records and databases, and equipment involved with these functions, with minimal disruption. The activation and relocation phase includes the following activities:

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

Activation and relocation plans or procedures should include the following:

1. A decision matrix for continuity of operations:
   a. With warning during duty hours and non-duty hours.
   b. Without warning during duty hours and non-duty hours.

2. Notification of:
   a. Continuity facilities team/site.
   b. Other POCs, as appropriate.
   c. Employees (continuity of operations essential personnel and non-deployed personnel).
3. Instructions on moving to a continuity facility, including directions to that site(s) and maps of routes from the primary location to the alternate or other continuity facility or location.
4. Identification of what drive-away kits should contain and how those kits will be maintained.
5. Instructions on moving vital records (those that have not been prepositioned) from the primary to the continuity facility.
6. Instructions on procuring necessary equipment/supplies that are not already in place.

Continuity Operations

This phase includes the following activities to continue essential functions:

1. Accounting for all organization personnel.
2. Conducting essential functions (which depend on the situation).
3. Establishing communications with supporting and supported organizations, customers, and stakeholders.
4. Conducting recovery activities as needed.

Plans or procedures should include:

1. Reception in-processing and accounting for continuity of operations personnel.
2. Transition of responsibilities to the deployed continuity of operations personnel.
3. Guidance for nondeployed personnel.

4. Identification of replacement personnel and augmentees, as necessary.
5. Execution of all essential functions at the continuity facility.
6. Activation of processes and procedures to acquire the resources necessary to continue essential functions and to sustain operations.
7. Notification of the adjacent organizations, customers, and stakeholders of continuity of operations activation and status.
8. Redeployment plans for phasing down continuity facility operations and returning operations, personnel, records, and equipment to the primary or other operating facility, when appropriate.

Reconstitution

Reconstitution is normally conducted using a priority-based phased approach, in which most essential functions are transferred last. Those functions that were discontinued because of the emergency should be reconstituted first. All personnel should be informed that the necessity for continuity of operations no longer exists. Instructions for resumption of normal operations are provided, including supervising an orderly return to the normal operating facility or moving to another temporary facility or to a new permanent facility. All organizations should report their location status to higher authority. The process of reconstitution will generally start immediately after an event concludes, and can run concurrently with the recovery process. Some of the activities involved with reconstitution include:

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

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

This page is intentionally left blank.

ANNEX O. ACRONYMS

AAR	After-Action Report
BIA	Business Impact Analysis
BPA	Business Process Analysis
CAG	Continuity Advisory Group
CAP	Corrective Action Program
CET	Continuity Evaluation Tool
CI/KR	Critical Infrastructure/Key Resources
COG	Continuity of Government
COGCON	Continuity of Government Readiness Conditions
COOP	Continuity of Operations
CWG	Continuity Working Group
DHS	Department of Homeland Security
ECG	Enduring Constitutional Government
ERG	Emergency Relocation Group
ESF	Emergency Support Function
FCD	Federal Continuity Directive
FEA	Federal Executive Association
FEB	Federal Executive Board
FEMA	Federal Emergency Management Agency
HQ	Headquarters
HSAS	Homeland Security Advisory System
HSEEP	Homeland Security Exercise and Evaluation Program
HSPD	Homeland Security Presidential Directive
IP	Improvement Plan
IT	Information Technology
MEF	Mission Essential Function
MOA/MOU	Memorandum of Agreement/Memorandum of Understanding
MYSPMP	Multi-Year Strategy and Program Management Plan
NCC	National Continuity Coordinator
NCP	National Continuity Programs
NCR	National Capital Region
NCS	National Communications System
NEF	National Essential Function
NEP	National Exercise Program
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan

NRF	National Response Framework
NSPD	National Security Presidential Directive
OEP	Occupant Emergency Plan
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSTP	Office of Science and Technology Policy
PMEF	Primary Mission Essential Function
POC	Point of Contact
SIP	Shelter-In-Place
TT&E	Test, Training, and Exercise
WMD	Weapons of Mass Destruction

ANNEX P. GLOSSARY

Activation – Once a Continuity of Operations plan has been implemented, whether in whole or in part, it is considered "activated."

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

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

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

Business impact analysis (BIA) – A method of identifying the effects of failing to perform a function or requirement.

Business process analysis (BPA) – A method of examining, identifying, and mapping the functional processes, workflows, activities, personnel expertise, systems, data, and facilities inherent in the execution of a function or requirement.

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

Category – This term refers to the categories of executive departments and agencies listed in Annex A to NSPD-51/HSPD-20 and Appendix B of the National Continuity Policy Implementation Plan.

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 MEFs.

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

Continuity capability – The ability of an organization to continue to perform its essential functions, using Continuity of Operations and COG programs and continuity requirements that have been integrated into the organization's daily operations, with the primary goal of ensuring the preservation of our form of government under the Constitution and the continuing performance of NEFs under all conditions. Building upon a foundation of continuity planning

and continuity program management, the pillars of a continuity capability are leadership, staff, communications, and facilities.

Continuity coordinators – At the Federal level these are representatives of executive branch departments and agencies at the assistant secretary (or equivalent) level. At the Non-Federal Entity level, these are the senior representatives tasked with coordinating the organizations continuity program.

Continuity of Government (COG) – A coordinated effort within the Federal Government's executive branch to ensure that NEFs continue to be performed during a catastrophic emergency.

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

Continuity of Operations event – Any event that causes an agency to relocate its operations to an alternate or other continuity site to assure continuance of its essential functions.

Continuity program management cycle – An ongoing, cyclical model of planning, training, evaluating, and implementing corrective actions for continuity capabilities.

Corrective action program (CAP) – The CAP system is a web-based application that allows Federal, State, territorial, tribal and local emergency response and homeland security officials to track and analyze improvements in their continuity plans and programs.

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

Critical infrastructure protection (CIP) – Risk management actions intended to prevent a threat or threat agent from attempting to, or succeeding at, destroying or incapacitating critical infrastructures.

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

Devolution – The capability to transfer statutory authority and responsibility for essential functions from an organization's primary operating staff and facilities to other organization employees and facilities, and to sustain that operational capability for an extended period.

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

Emergency coordinator – The key senior official appointed within an organizational element or higher, who serves as the coordinator for all National Response Framework (NRF) and National Incident Management System (NIMS) continuity of operations related issues.

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

Emergency Relocation Group (ERG) – Pre-designated staff who move to a relocation site to continue essential functions in the event that their normal work locations are threatened or have been incapacitated by an incident. The ERG is composed of an advance team plus emergency personnel.

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

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

Essential resources – Resources that support the organization's ability to provide vital services, exercise civil authority, maintain the safety and well-being of the general populace, and sustain the Nation's industrial and economic bases during an emergency.

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

Federal Continuity Directive (FCD) – A document developed and promulgated by DHS, in coordination with the Continuity Advisory Group (CAG) and in consultation with the Continuity Policy Coordination Committee (CPCC), which directs Federal 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 (FEBs), for communication and collaboration among Federal agencies outside of Washington, DC, utilized to help coordinate the field activities of Federal departments and agencies in localized sections of the Nation.

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

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

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

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

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

Improvement Plan (IP) – A cycle of events that incorporates evaluations, AARs, and lessons learned into the development and implementation of an IP.

Interagency agreements – A written agreement entered into between agencies that require specific goods or services to be furnished or tasks to be accomplished by one agency in support of the other.

Interoperability – "Interoperability" has two meanings: (1) The ability of systems, personnel, or agencies to provide services to and accept services from other systems, personnel, or agencies, and to use the services so exchanged so that these organizations can operate together effectively; (2) A condition that is realized among electronic-communications operating systems or grids and/or among individual electronic-communications devices, when those systems and/or devices allow the direct, seamless, and satisfactory exchange of information and services between the users of those systems and devices.

Continuity communications – Communications that provide the capability to perform essential functions, in conjunction with other organizations until normal operations can be resumed.

Leadership – The senior decision makers who have been elected (e.g., the President, State governors) or designated (e.g., Cabinet Secretaries, chief executive officers) to head a branch of Government or other organization. The survivability of leadership is accomplished by physically protecting the officeholder (sheltering the individual in place or relocating him or her away from the threat area) and by developing a prioritized list of designated successors to that leadership position, who would assume the roles and responsibilities of that position in the event of the incapacitation or unavailability of the current officeholder. The designation as a successor enables an individual to act for the officeholder and exercise the powers and authorities of the officeholder's position, in the event of the officeholder's death, permanent disability, or resignation.

Legal and financial records – Records that are necessary to protect the legal and financial rights of both the government and private sector and the persons who are affected by its actions.

Mission-critical data – Information essential to supporting the execution of an organization's essential functions.

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

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

National Communications System (NCS) – An organization within DHS, the NCS assists the President, the National Security Council (NSC), the Homeland Security Council (HSC), the Director of the Office of Science and Technology Policy (OSTP), and the Director of the Office of Management and Budget (OMB) in (1) the exercise of telecommunications functions and their associated responsibilities and (2) the coordination of planning for providing the Federal Government, under all circumstances (including crises and emergencies, attacks, and recovery and reconstitution from those events), with the requisite national-security and emergency-preparedness communications resources.

National Continuity Policy – Establishes a comprehensive national course of action for the continuity of Government and supporting private sector structures and operations.

National Essential Functions (NEFs) – The eight functions the President and the Nation's leadership will focus on to lead and sustain the Nation during a catastrophic emergency; NEFs, therefore, should be supported by COOP and COG capabilities.

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

Non-Federal Entities – The State, local, territorial, and tribal governments, and private sector organizations are referred to as non-federal entities.

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

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

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

Plan – A proposed or intended method of getting from one set of circumstances to another. A plan is often used to move from the present situation towards the achievement of one or more objectives or goals.

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

Primary Mission Essential Functions (PMEFs) – Those department and agency Mission Essential Functions, validated by the NCC, which should 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.

Reconstitution – The process by which surviving and or replacement organization personnel resume normal agency operations from the original or replacement primary operating facility.

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

Risk analysis – The process by which risks are identified and evaluated.

Risk assessment – The identification and assessment of hazards.

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

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

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

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

Telework – The ability to work at a location other than the official duty station, using portable computers, high-speed telecommunications links, and mobile communications devices.

Test, Training, and Exercise (TT&E) Program – Measures to ensure that an organization's continuity plan is capable of supporting the continued execution of the organization's essential functions throughout the duration of a continuity situation.

Virtual offices – A location or environment where employees use portable information technologies and communication packages to do their work.

Vital databases – Information systems that are needed to support essential functions during a continuity situation.

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

Vulnerability analysis – A process that defines, identifies, and classifies the susceptibility of a facility, computer, network, or communications infrastructure, to damage or destruction. In addition, a vulnerability analysis can forecast the effectiveness of proposed countermeasures and can evaluate their actual effectiveness after they are implemented.

Warm Site – A continuity facility that is equipped with some hardware, and communications interfaces, electrical and environmental conditioning which is capable of providing backup after additional provisioning, software or customization is performed.

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

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

This page is intentionally left blank.

ANNEX Q. AUTHORITIES AND REFERENCES

The following are the authorities and references for this CGC 1:

AUTHORITIES:

1) The National Security Act of 1947, dated July 26, 1947, as amended.
2) The Homeland Security Act of 2002 (Public Law 107-296), dated November 25, 2002.
3) Executive Order 12148, Federal Emergency Management, dated July 20, 1979, as amended.
4) Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, dated April 3, 1984, as amended.
5) Executive Order 12656, Assignment of Emergency Preparedness Responsibilities, dated November 18, 1988, as amended.
6) Executive Order 13286, Establishing the Office of Homeland Security, dated February 28, 2003.
7) National Security Presidential Directive 51/Homeland Security Presidential Directive 20, National Continuity Policy, dated May 9, 2007.
8) Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection, dated December 17, 2003.
9) Homeland Security Presidential Directive 8, National Preparedness, dated December 17, 2003.
10) Homeland Security Presidential Directive 8 Annex 1, National Planning, dated September 9, 2008.
11) National Continuity Policy Implementation Plan, dated August 2007.
12) National Communications System Directive 3-10, Minimum Requirements for Continuity Communications Capabilities, dated July 25, 2007.

REFERENCES:

1) 36 Code of Federal Regulations, Part 1236, Management of Vital Records, revised as of July 1, 2000.
2) 41 Code of Federal Regulations 101.20.103-4, Occupant Emergency Program, revised as of July 1, 2000.
3) Presidential Decision Directive 62, Protection Against Unconventional Threats to the Homeland and Americans Overseas, dated May 22, 1998.
4) Homeland Security Presidential Directive 1, Organization and Operation of the Homeland Security Council, dated October 29, 2001.

5) Homeland Security Presidential Directive 3, Homeland Security Advisory System, dated March 11, 2002.
6) Homeland Security Presidential Directive 5, Management of Domestic Incidents, dated February 28, 2003.
7) Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, dated August 27, 2004.
8) National Infrastructure Protection Plan, dated 2006.
9) National Strategy for Pandemic Influenza, dated November 1, 2005.
10) National Strategy for Pandemic Influenza Implementation Plan, dated May 2006.
11) National Exercise Program Implementation Plan, April 2007.
12) National Incident Management System (NIMS), dated March 1, 2004.
13) NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, dated June 2002.
14) NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, dated December 2006.
15) NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs, 2007 Edition.
16) Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements, dated February 2008
17) Federal Continuity Directive 2, Federal Executive Branch Mission Essential Function and Primary Mission Essential Function Identification and Submission Process, dated February 2008

This page is intentionally left blank