

**U.S. Department of Energy
Cyber Security Program**

**CONTINGENCY PLANNING
GUIDANCE**



August 31, 2006

***This Guidance document was
developed and issued outside of the
Departmental Directives Program.***

1. PURPOSE.

This Department of Energy (DOE) Chief Information Officer (CIO) Guidance provides guidance for the implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, *Contingency Planning Guide for Information Technology Systems*, within the DOE, including the National Nuclear Security Administration (NNSA).

Contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of systems, operations, and data after a disruption. Contingency planning generally includes one or more of the approaches to restore disrupted services:

- Restoring operations at an alternate location,
- Recovering operations using alternate equipment, or
- Performing some or all of the affected business processes using alternate means.

Contingency planning establishes the plans, procedures, and technical measures that can enable a system to be resistant to disruption and recovered quickly and effectively following a service disruption or disaster. Although contingency planning is associated with activities occurring in the Continuous Monitoring Phase of the Certification and Accreditation (C&A) process, contingency measures should be identified and integrated at all phases of the C&A process. This approach reduces overall contingency planning costs, enhances contingency capabilities, and reduces impacts to system operations when the contingency plan is activated. Contingency planning for information systems is an integral part, but not the primary focus, of operating unit planning for Continuity of Operations, Business Continuity, Business Recovery, Disaster Recovery, or Occupant Emergency.

This Guidance is provided to Senior DOE Management for addressing the controls in DOE CIO Guidance CS-1, *Management, Operations, and Technical Controls Guidance*, DOE CIO Guidance CS-22, *National Security Systems Controls Guidance*, in their Program Cyber Security Plans (PCSPs), and additional controls resulting from an operating unit risk assessment. Specifically, this Guidance applies to controls CP-1, CP-2, CP-3, CP-4, CP-5, CP-6, CP-7, CP-8, CP-9, and CP-10 in CS-1 and ENV_AVA.1 and ENV_RCV.1 in CS-22.

The DOE Office of the Chief Information Officer (OCIO) will review this Guidance annually and update it as necessary. The DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE Chief Information Officer (CIO) (hereinafter referred to as Senior DOE Management) and their subordinate organizations and contractors (hereinafter called operating units) may provide feedback at any time for incorporation into the next scheduled update.

2. CANCELLATIONS.

None.

3. APPLICABILITY.

- a. Primary DOE Organizations. This Guidance applies to all DOE Organizations listed in Attachment 1, *Primary Department of Energy Organizations to which DOE CIO Guidance CS-7 is Applicable.*

Further, Senior DOE Management may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their operating units, and for ensuring that those requirements are incorporated into contracts.

- b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Guidance for activities under the NNSA Administrator's cognizance.
- c. DOE Unclassified Systems. Senior DOE Management PCSPs are to address this Guidance for all systems hosting unclassified information. DOE CIO Guidance CS-38, *Protection of Personally Identifiable Information*, DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, provides additional information for identifying unclassified information requiring protection.
- d. National Security Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE National Security Systems. The protection mechanisms described in this guidance are consistent with and implement the policies and practices set forth by Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program; the requirements of the *National Industrial Security Program Operating Manual (NISPOM)*; the Atomic Energy Act of 1954, which established Restricted Data information; and EO 12958, *Classified National Security Information*, which prescribes a uniform system for classifying, safeguarding, and declassifying national security information.. NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, provides additional guidance for identifying National Security systems.

4. IMPLEMENTATION.

This Guidance is effective 30 days after issuance. However, DOE recognizes that this Guidance cannot be implemented into Senior DOE Management Program Cyber Security Plans (PCSPs) overnight. Except as noted below, DOE expects that Senior DOE Management shall address the criteria in this document within 90 days of its issuance. If Senior DOE Management cannot address all of the criteria by that date, Senior DOE Management are to establish a Plan of Actions and Milestones (POA&M) for implementation of this Guidance into their PCSPs.

5. CRITERIA.

- a. Program Cyber Security Plans. Senior DOE Management PCSPs are to be consistent with the criteria in DOE OCIO Guidance CS-1, *Management, Operational, and Technical Controls*. To ensure consistency with these controls, Senior DOE Management PCSPs are to direct operating units to develop, document, and implement contingency planning policies and procedures consistent with the following criteria and commensurate with the level of security required for the organization's environment and specific needs.
 - (1) Accomplish planning and documentation for contingencies, as described below for each information system during the information system C&A process.
 - (2) Implement and test contingency plans for all information systems.
 - (3) Provide contingency plan test reports on Critical Infrastructure and Key Resources to Senior DOE Management.
 - (4) Ensure the availability of information systems within the time frames designated in the PCSP.
 - (5) Assign the following responsibilities to specific roles in the applicable PCSP.
 - (a) Management Responsibilities.
 - i. Develop contingency planning policy statement for the operating unit.
 - ii. Distribute the policy statement to management staff for implementation.
 - iii. Ensure resources are available to implement and test contingency plans.
 - iv. Determine authority to activate contingency plan(s).
 - (b) Contingency Planning Responsibilities.
 - i. Manage the development, testing, test reporting, and execution of Contingency Plans.
 - ii. Provide Contingency Plan test reports to Senior DOE Management for Critical Infrastructure and Key Resource systems, systems critical to the safety and health of employees and the public, and systems critical in maintaining commitments to external organizations.
 - iii. Review contingency plan(s) at least annually and update as necessary.
 - iv. Prepare POA&Ms for contingency planning as necessary.
 - v. Conduct Business Impact Analyses (BIAs).

- vi. Determine recovery strategy(ies) in coordination with users and Information System Owners.
 - vii. Coordinate contingency planning with Emergency Management, Disaster Recovery planners, and other activities dependent on the information system.
 - viii. Coordinate contingency plans with external organizations and System Owners to ensure that impacts caused by changes within either organization will be reflected in the contingency plan.
 - ix. Designate teams to implement contingency strategy(ies).
- (6) Identify Information Owner/ Data Steward responsibilities as follows:
- (a) Ensure applications and/ or data supporting Critical Infrastructure or Key Resources are identified.
 - (b) Provide resources to support the implementation and testing of contingency plans for the application and data.
- (7) Identify Information System Owner/ Program Manager responsibilities as follows:
- (a) Act as the Point-of-Contact for coordinating contingency requirements of all applications hosted by the system.
 - (b) Ensure the resources for implementation of Contingency Plans for their systems are identified.
 - (c) Test and prepare test reports on the Contingency Plan for his/her information system.
- b. Contingency Planning. Senior DOE Management PCSPs are to describe the contingency planning process for operating units to include the following.
- (1) Operating Unit Policy. Define overall contingency objectives, establish the framework (e.g., roles and responsibilities, resource and training requirements, exercise, maintenance, and test schedules, etc.), and criteria (safety of personnel; extent of damage to the site, facility, or system; criticality of the system to the operating unit's mission, and anticipated disruption; etc.) for activating the contingency plan(s).
 - (2) Business Impact Analyses (BIAs). Conduct BIAs to identify systems providing critical services and prioritize these systems and their components. These BIAs should fully characterize the system requirements, processes, and interdependencies to determine contingency requirements and priorities. The BIA for Critical Infrastructure or Key Resource systems may be limited to a determination of critical components needed to maintain essential operation. The BIAs for the remaining

systems under the purview of the operating unit are to include all elements of the BIA. The BIA process is description follows:

- (a) Identify critical information system resources.
 - i. Identify data users, providers, and flows
 - ii. Identify the system components and infrastructure (electric power, servers, routers, authentication servers, etc) required to extract or enter data.
 - (b) Identify disruption impacts and allowable outage times.
 - i. Identify the magnitude of expected disruptions from operating unit-level plans, such as Disaster Recovery, Continuity of Operations, and Occupant Emergency Plans, to determine the threats from natural, human, or environmental sources.
 - ii. Identify the maximum allowable time the system or system component may be unavailable before it prevents a mission-essential function from being performed.
 - iii. Identify any related or dependent systems and processes that will be disrupted by the unavailability of the system.
 - iv. Identify the point in time where the cost of system inoperability and the cost of restoration are equal.
 - (c) Develop recovery priorities.
 - i. Use the data obtained from previous activities to prioritize recovery for systems and system components.
 - ii. Determine the recovery time line for each system component.
 - iii. Initiate the preparation of Plans of Action and Milestones (POA&Ms) for any systems that are prioritized below current funding capabilities.
- (3) Preventive Controls. Identify measures taken or to be taken to reduce the effects of system disruptions.
- (a) Identify the vulnerabilities to natural, human, or environmental threats.
 - (b) Develop mitigation strategies to reduce or eliminate impacts to system components, in priority order, based on the BIAs.
 - (c) Update Plans of Action and Milestones (POA&Ms) for any system that is prioritized below current funding capabilities.

- (4) Recovery Strategies. Develop thorough recovery strategies to ensure that the system may be recovered as effectively and as quickly as needed following a disruption.
- (a) Identify the threats and/or vulnerabilities that could not be mitigated.
 - (b) Develop recovery strategies based on the disruption impacts and the allowable outage times from the BIAs.
 - (c) Identify those personnel or teams to accomplish the decision making, coordination, administrative, and technical functions required for contingency plan execution such as:
 - i. Senior Management Official
 - ii. Management
 - iii. Damage Assessment
 - iv. Alternate Site Recovery Coordination
 - v. Hardware Salvage
 - vi. Data Recovery
 - vii. Database Recovery
 - viii. Application Recovery
 - ix. LAN/WAN Recovery
 - x. Telecommunications
 - xi. Network Operations Recovery
 - xii. Software and Data Recovery
 - xiii. System Software
 - xiv. Operating System Administration
 - xv. System Recovery
 - xvi. Server Recovery
 - xvii. Administrative Support
 - xviii. Original Site Restoration/Salvage Coordination
 - xix. Test

xx. Procurement (equipment and supplies)

xxi. Physical/Personnel Security

xxii. Transportation and Relocation

xxiii. Media Relations

xxiv. Legal Affairs

(d) Update the POA&M to include resource requirements to implement this portion of the Contingency Plan.

(5) Testing, training, and exercises.

(a) Testing

i. The results of all testing must be documented in a test report.

ii. Test reports for Critical Infrastructure and Key Resource information systems must be forwarded to the cognizant Senior DOE Management official.

iii. Testing may take two forms.

- Tabletop Exercise –A Tabletop Exercise of all contingency plans must be conducted annually.
- Functional Exercise –A Functional Exercise of Critical Infrastructure and Key Resource contingency plans must be conducted annually and all other information systems bi-annually to include the elements of Notification/Activation, Recovery, and Reconstitution, as a minimum.

iv. POA&M Update – Update the POA&M to include resource requirements to implement this portion of the Contingency Plan.

(b) Training –Training will be accomplished annually and as part of changes to the contingency plan. The following plan elements shall be included in training:

i. Purpose of the plan

ii. Cross-team coordination and communication

iii. Reporting procedures

iv. Security requirements

- v. Team-specific processes such as notification/ activation, recovery, and reconstitution
 - vi. Individual responsibilities in contingency processes
 - vii. POA&M Update – Update the POA&M to include resource requirements to implement this portion of the Contingency Plan.
- (6) Plan maintenance. The plan is a living document that is reviewed and updated, if changes have occurred, annually to remain current with system enhancements, results of plan testing, team staffing changes, and changes in organization priorities. The contingency plan shall be a configuration item and maintained as part of the System Security Plan (SSP). A change to the system or its environment, which includes the contingency plan elements, requires the modified SSP to be approved prior to implementing the changes.
- c. Contingency Plan Development. The contingency plan should be tailored to the operating unit and its requirements and is an important element of the certification and accreditation package. The plan contains detailed roles, responsibilities, teams, and procedures associated with restoring an information system and documents technical capabilities designed to support contingency operations. The following identified contingency plan outline provides an example of how a plan may be constructed.
- (1) Introduction. The Introduction includes background and contextual information that makes the contingency plan easier to understand, implement, and maintain and to orient the reader to the type and location of information contained in the plan.
- (a) Purpose. This subsection establishes the reason for writing the plan.
 - (b) Applicability. The organization(s) impacted by the contingency plan is documented and the relationship to any other plans supporting or supported by the plan, such as Emergency Management Plans, is described.
 - (c) Scope. This section discusses the issues, situations, and conditions addressed and not addressed in the contingency plan. The types of contingency situations the plan is intended to cover should be discussed. These situations may range from a temporary loss of commercial power to disaster recovery operations. The system, location(s) for the system or system components covered, and any assumptions are described.
 - (d) References/Requirements. This subsection identifies the DOE, Senior DOE Management, and operating unit requirements for contingency planning.
 - (e) Record of Changes. This subsection describes the configuration history of the contingency plan by recording dates, version, and reason for contingency plan changes.

- (2) Concept of Operations. The Concept of Operations element provides additional detail about the system, planning framework, response activities, recovery activities, and resumption activities.
- (a) System Description. The description should include the system architecture, location(s), internal and external connections, security components, and any other technical detail that would assist the contingency teams in understanding the system configuration and operation.
 - (b) Line of Succession. The order of succession identifies the personnel responsible for assuming authority in the event the designated person is unavailable.
 - (c) Responsibilities. This subsection describes the overall structure of the contingency teams. The coordination mechanisms and requirements as well as an overview of team member roles and responsibilities are described.
- (3) Notification/Activation. The Notification/Activation element defines the initial actions to be accomplished to notify personnel, assess damage, and implement the plan once a disruption or emergency has been detected or is expected.
- (a) Notification Procedures. The procedures should describe the methods of notification under various contingency scenarios. The method(s) of notification of each team member must take into account the possibilities of widespread disasters, the ability to contact personnel on short notice during and after business hours, and the necessity to contact alternate personnel.
 - (b) Damage Assessment. In order to appropriately implement the contingency plan, the nature and extent of damage must be assessed as early as possible. Personnel performing damage assessment must be sufficiently trained in their part(s) of these procedures that performance can be accomplished without written procedures available. Specific damage assessment procedures may be unique to each system, but the following areas must be addressed:
 - i. The cause of the emergency or disruption,
 - ii. The potential for additional disruptions or damage,
 - iii. Area affected by the emergency,
 - iv. Status of physical infrastructure (e.g. structural integrity of building/room, electric power availability, HVAC, and telecommunications),
 - v. Inventory and functional status of system components,
 - vi. Type of damage to system components (e.g. water, fire and heat, physical, and electric surge),

- vii. System components to be replaced, and
 - viii. Estimated time required to restore normal system operation.
- (c) Plan Activation. The Contingency Planning Coordinator evaluates the result of the damage assessment against the plan activation criteria and determines the strategy to be used if the plan is to be activated. The detailed activation criteria are located in this section of the plan and cover personnel safety, extent of damage to the facility, extent of damage to the system, criticality to the operating unit's mission, and anticipated duration of disruption.
- (4) Recovery. The Recovery element includes the operations that begin after the contingency plan has been activated, damage assessment has been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery activities focus on contingency measures to execute temporary processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility. At the completion of the Recovery Phase, the system will be operational and performing the functions designated in the plan.
- (a) Recovery Sequence. The sequence of activities should reflect the system's allowable outage time to avoid significant impacts to related systems and their application. Procedures should be written in a stepwise, sequential format so system components can be restored in a logical manner. The most critical items to restoring service and the system foundation items should be recovered first. The procedures must include coordination activities with other teams or external organizations that are dependent on completion of certain steps, such as when time frames are not being met, a step has been completed that allows another team to proceed, or items must be procured.
- (b) Recovery Procedures. Recovery procedures are to be written that allow personnel unfamiliar with the site, facility, or system configuration to perform the recovery. Recovery procedures are to include date and time of step completion and the name of the team member who completed it. Particular procedures are to be assigned to the appropriate recovery team and address the following:
- i. Obtaining approval to access the damaged facilities or areas,
 - ii. Notifying internal and external organizations associated with the system,
 - iii. Obtaining office supplies and work space,
 - iv. Obtaining and installing hardware,
 - v. Obtaining backup media,
 - vi. Restoring operating and application software,

- vii. Restoring system and application data,
 - viii. Testing system functionality and security,
 - ix. Notification to user(s), and
 - x. Operating alternate equipment.
- (5) Reconstitution. Once the original or new site/facility is restored to the level that it can support the system and its normal processes, the system may be transitioned back to the original or to the new site/facility. Until the primary system is restored and tested, the contingency system should continue to be operated. The plan should specify teams responsible for restoring or replacing both the facility and the system. The following major activities are addressed:
- (a) Ensuring adequate infrastructure support, such as electric power, water, telecommunications, security, environmental controls, office equipment, and supplies;
 - (b) Installing system hardware, software, and firmware. This activity should include detailed restoration procedures similar to those followed in Recovery;
 - (c) Establishing connectivity and interfaces with network components and external systems;
 - (d) Testing system operations and security to ensure full functionality;
 - (e) Backing up operational data on the contingency system and uploading to restored system;
 - (f) Shutting down the contingency system;
 - (g) Terminating contingency operations;
 - (h) Securing, removing, and/or relocating all sensitive materials at the contingency site; and
 - (i) Arranging for recovery personnel to return to the original facility.
- d. Contingency Plan Structure. Senior DOE Management PCSPs are to require operating units to have the minimum content shown in the following sections. The structure of a contingency plan is based on the importance of systems for which the plan is written. The following sections describe the minimum contingency plan elements based on the designation of the system. Table 1 summarizes the required content of the contingency plan for the different types of systems.
- (1) Critical Infrastructure. Critical Infrastructure contingency plans must address each of the elements described in the paragraph 3 in sufficient detail to allow technically

competent personnel unfamiliar with the system to create and operate the contingency system in a different location.

- (2) Key Resources. Key Resources contingency plans must address each of the elements indicated in the following section in sufficient detail for personnel familiar with the system to create and operate the contingency system in a different location.
 - (a) Introduction
 - (b) Scope
 - (c) Concept of Operations
 - (d) Notification/Activation
 - (e) Recovery Procedures
 - (f) Reconstitution
- (3) Other Systems. Contingency plans for all other types of systems must address each element listed below in sufficient detail to allow personnel who normally operate the systems to restore operations.
 - (a) Introduction
 - i. Scope
 - (b) Concept of Operations
 - i. System Description
 - ii. Line of Succession
 - (c) Notification/Activation
 - i. Notification Procedures
 - ii. Plan Activation
 - (d) Recovery Procedures
 - i. Hardware Installation
 - ii. Backup Media
 - iii. Software Restoration
 - iv. Functional and Security Testing

- v. User Notification
- (e) Reconstitution
 - i. Infrastructure Support
 - ii. Internal and External Networking
 - iii. Functional and Security Testing

Table 1 Contingency Plan Structure

Plan Content [Guidance Section]	Critical Infrastructure Systems	Key Resource Systems	Other Systems
Introduction [5.c.(1)]			
Purpose [5.c.(1)(a)]	X		
Applicability [5.c.(1)(b)]	X		
Scope [5.c.(1)(c)]	X	X	X
References/Requirements [5.c.(1)(d)]	X		
Record of Changes [5.c.(1)(e)]	X		
Concept of Operations [5.c.(2)]			
System Description [5.c.(2)(a)]	X	X	X
Line of Succession [5.c.(2)(b)]	X	X	X
Responsibilities [5.c.(2)(c)]	X	X	
Notification/Activation [5.c.(3)]			
Notification Procedures [5.c.(3)(a)]	X	X	X
Damage Assessment [5.c.(3)(b)]	X	X	
Plan Activation [5.c.(3)(c)]	X	X	X
Recovery [5.c.(4)]			
Recovery Sequence [5.c.(4)(a)]	X		
Recovery Procedures [5.c.(4)(b)]	X	X	X
Facility Access [5.c.(4)(b)i]	X	X	
Internal/External Notification [5.c.(4)(b)ii]	X	X	
Administrative Support [5.c.(4)(b)iii]	X	X	
Hardware Installation [5.c.(4)(b)iv]	X	X	X
Media Backup [5.c.(4)(b)v]	X	X	X
Software Restoration [5.c.(4)(b)vi]	X	X	X
Data Restoration [5.c.(4)(b)vii]	X	X	
Functional and Security Testing [5.c.(4)(b)viii]	X	X	X
User Notification [5.c.(4)(b)ix]	X	X	X
Operating Equipment [5.c.(4)(b)x]	X	X	X
Reconstitution [5.c.(5)]			
Infrastructure Support [5.c.(5)(a)]	X	X	X
Hardware/Software Installation [5.c.(5)(b)]	X	X	
Internal and External Networking [5.c.(5)(c)]	X	X	X
Functional and Security Testing [5.c.(5)(d)]	X	X	X
Data Restoration [5.c.(5)(e)]	X	X	
Contingency Shutdown [5.c.(5)(f)]	X	X	
Contingency Termination [5.c.(5)(g)]	X	X	
Securing Contingency Site [5.c.(5)(h)]	X	X	
Personnel Return [5.c.(5)(i)]	X	X	

6. REFERENCES.

References are listed in DOE CIO Guidance CS-1, *Management, Operations, and Technical Controls Guidance*.

7. DEFINITIONS.

Terms specific to this Guidance are defined in Attachment 2. Acronyms and terms applicable to all DOE CIO Guidance are defined in DOE CIO Guidance CS-1, *Management, Operations, and Technical Controls Guidance*.

8. CONTACT.

Questions concerning this Guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

ATTACHMENT 1

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH DOE CIO
GUIDANCE CS-7 IS APPLICABLE

Office of the Secretary
Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Human Capital Management
Office of the Inspector General
Office of Intelligence and Counterintelligence
Office of Legacy Management
Office of Management
National Nuclear Security Administration
Office of Nuclear Energy
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Office of Security and Safety Performance Assurance
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

ATTACHMENT 2

GLOSSARY

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

Data Steward. The person acting on behalf of the data owner for the generation, management, and destruction of data and to ensure the review of information sensitivity and classification.

Key Resources. Publicly or privately controlled resources essential to the minimal operations of the economy and government.