Contingency Planning (TMR-7)
October 10, 2007

Department of Energy (DOE) Order 205.1A, *Department of Energy Cyber Security Management*, charges Senior DOE Management to implement cyber security within their respective organizations, based on their determination, assessment, and documentation of DOE and program-unique threats and risks. In carrying out this charge, Senior DOE Management is required by the Order to develop a Program Cyber Security Plan (PCSP) that defines cyber security requirements for all subordinate organizations and programs. The Order requires that the PCSP requirements comply with the Federal Information Security Management Act (FISMA), Presidential directives and Executive orders, Office of Management and Budget (OMB) directives, Federal Information Processing Standards (FIPS), Departmental policies, and DOE Chief Information Officer (CIO) Cyber Security Technical and Management Requirements (TMRs). This TMR document provides Senior DOE Management general direction and minimum requirements for unclassified and National Security Systems to be used in preparing each PCSP.

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 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. This TMR establishes a risk-based approach to contingency planning that is to be covered in each PCSP for information systems within the DOE. It also provides for the Departmental implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, *Contingency Planning Guide for Information Technology Systems,* and contingency planning requirements as defined by OMB in annual FISMA reporting guidance. Senior DOE Management may specify and implement additional requirements in the PCSP to address specific risks, vulnerabilities, or threats within its operating units.

Cancellations

This TMR replaces DOE CIO Guidance CS-7, *Contingency Planning Guidance*, dated August 31, 2006.

Implementation

This document defines management and technical cyber security requirements to be incorporated into Senior DOE Management PCSPs within 90 days of the TMR issue date.

Requirements

TMR-7-1, Senior DOE Management Contingency Planning Processes

Senior DOE Management is responsible for developing, documenting in the PCSP, and implementing contingency planning processes for all operating units, programs, and

systems covered under the organization's PCSP. The Senior DOE Management PCSP is to describe the contingency planning process 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 (e.g., safety of personnel; extent of damage to the site, facility, or system; criticality of the system to the operating unit or Senior DOE Management mission; anticipated disruption; etc.) for activating the contingency plan(s). Operating unit policy is to:

    a. Accomplish planning and documentation for contingencies, as described in TMR-7-2 for each information system during the C&A process. The plan is to be reviewed annually and updated to remain current with system enhancements, results of plan testing, team staffing changes, and changes in organization priorities.

    b. Implement and test contingency plans for all information systems.

    c. Provide contingency plan test reports on Critical Infrastructure and Key Resources to Senior DOE Management.

    d. Ensure the availability of information systems are within the Operating Unit or Senior DOE Management mission-requirement time frames.

    e. Assign responsibilities.

        (1) Management Responsibilities.

            (a) Develop contingency planning policy statement for the operating unit.

            (b) Distribute the policy statement to management staff for implementation.

            (c) Ensure resources are available to implement and test contingency plans.

            (d) Determine authority to activate contingency plan(s).

        (2) Contingency Planning Responsibilities.

            (a) Manage the development, testing, test reporting, and execution of Contingency Plans.

            (b) 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.

(c) Review contingency plan(s) at least annually and update as necessary.

(d) Prepare POA&Ms for contingency planning as necessary.

(e) Conduct Business Impact Analyses (BIAs).

(f) Determine recovery strategy(ies) in coordination with users and System Owners.

(g) Coordinate contingency planning with Emergency Management, Disaster Recovery planners, and other activities dependent on the information system.

(h) 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.

(i) Designate teams to implement contingency strategy(ies).

(3) 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.

(4) Identify System Owner 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.

2. Business Impact Analyses (BIAs). Conduct BIAs to identify systems providing critical services and prioritize systems and their components. The BIAs should fully

characterize the system requirements, processes, and interdependencies to determine contingency requirements and priorities.[1] The BIA process should include:

a. Identify critical information system resources.

(1) Data users, providers, and flows.

(2) System components and infrastructure (e.g., electric power, servers, routers, authentication servers, etc.) required to extract or enter data.

b. Identify disruption impacts and allowable outage times, including:

(1) The magnitude of expected disruptions from operating unit-level plans (e.g., Disaster Recovery, Continuity of Operations, and Occupant Emergency Plans).

(2) The maximum allowable time the system or system component may be unavailable before it prevents a mission-essential function from being performed.

(3) Any related or dependent systems and processes that will be disrupted by the unavailability of the system.

(4) The point where cost of system inoperability equals cost of restoration.

c. Develop recovery priorities.

(1) Use the data obtained from previous activities to prioritize recovery for systems and system components.

(2) Determine the recovery time line for each system component.

(3) Create a Plan of Action and Milestones (POA&M) 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.

---

[1] The BIA for Critical Infrastructure or Key Resource systems may be limited to a determination of critical components needed to maintain essential operation.

c. Create or update a POA&M as necessary 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 efficiently and 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 personnel or teams to accomplish the decision making, coordination, administrative, and technical functions required for contingency plan execution.

   d. Create or update a POA&M as necessary to include resource requirements to implement this portion of the Contingency Plan.

5. Testing, training, and exercises. Contingency plan testing is intended to ensure that all personnel involved know the actions they are to accomplish in a contingency situation and that the contingency plan is up to date with any changes in the system. If a disruptive event has occurred and the contingency plan was activated between tests, the next test may be extended from the date of event recovery.

   a. Testing.

      (1) The results of all testing must be documented in a test report.

      (2) Test reports for Critical Infrastructure and Key Resources must be forwarded to the cognizant Senior DOE Management official.

      (3) Testing may take two forms.

         (a) Tabletop Exercise –A Tabletop Exercise of all contingency plans must be conducted annually when a Functional Exercise is not conducted.

         (b) Functional Exercise –A Functional Exercise of Critical Infrastructure and Key Resource contingency plans must be conducted annually and all **Moderate and High category** information systems at least every 2 years to include the elements of Notification/Activation, Recovery, and Reconstitution, as a minimum.

      (4) Create or update a POA&M as necessary 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.

(1) Include the following elements in the Training Plan:

(a) Purpose of the plan.

(b) Cross-team coordination and communication.

(c) Reporting procedures.

(d) Security requirements.

(e) Team-specific processes such as notification/ activation, recovery, and reconstitution.

(f) Individual responsibilities in contingency processes.

(2) Create or update a POA&M as necessary to include resource requirements to implement this portion of the Contingency Plan.

TMR-7-2, Contingency Plan Contents

The Senior DOE Management PCSP is to require operating units to have the minimum Contingency Plan 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, should be tailored to the operating unit and its requirements, and is maintained as part of the C&A Package. Critical Infrastructure and Key Resources contingency plans must address each of the identified elements in sufficient detail to allow technically competent personnel unfamiliar with the system to create and operate at a different location. 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. Table 1 identifies the required content of the contingency plan for the different types of systems.

Table 1, Contingency Plan Structure

Plan Content [TMR-7-2 Section]	Critical Infrastructure Systems	Key Resource Systems	Other Systems
Introduction [1]			
Purpose [1.a.]	X		
Applicability [1.b]	X		
Scope [1.c]	X	X	X
References/Requirements [1.d]	X		
Record of Changes [1.e]	X		
Concept of Operations [2]			

Plan Content [TMR-7-2 Section]	Critical Infrastructure Systems	Key Resource Systems	Other Systems
System Description [2.a]	X	X	X
Line of Succession [2.b]	X	X	X
Responsibilities [2.c]	X	X	
Notification/Activation [3]			
Notification Procedures [3.a]	X	X	X
Damage Assessment [3.b]	X	X	
Plan Activation [3.c]	X	X	X
Recovery [4]			
Recovery Sequence [4.a]	X		
Recovery Procedures [4.b]	X	X	X
Facility Access [4.b.(1)]	X	X	
Internal/External Notification [4.b.(2)]	X	X	
Administrative Support [4.b.(3)]	X	X	
Hardware Installation [4.b.(4)]	X	X	X
Media Backup [4.b.(5)]	X	X	X
Software Restoration [4.b.(6)]	X	X	X
Data Restoration [4.b.(7)]	X	X	
Functional and Security Testing [4.b.(8)]	X	X	X
User Notification [4.b.(9)]	X	X	X
Operating Equipment [4.b.(10)]	X	X	X
Reconstitution [5]			
Infrastructure Support [5.a]	X	X	X
Hardware/Software Installation [5.b]	X	X	
Internal and External Networking [5.c]	X	X	X
Functional and Security Testing [5.d]	X	X	X
Data Restoration [5.e]	X	X	
Contingency Shutdown [5.f]	X	X	
Contingency Termination [5.g]	X	X	
Securing Contingency Site [5.h]	X	X	
Personnel Return [5.i]	X	X	

The following sections describe contingency plan elements and content.

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:

(1) The cause of the emergency or disruption,

(2) The potential for additional disruptions or damage,

(3) Area affected by the emergency,

(4) Status of physical infrastructure (e.g. structural integrity of building/room, electric power availability, HVAC, and telecommunications),

(5) Inventory and functional status of system components,

(6) Type of damage to system components (e.g. water, fire and heat, physical, and electric surge),

(7) System components to be replaced, and

(8) Estimated time required to restore normal system operation.

c. Plan Activation. 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:

(1) Obtaining approval to access the damaged facilities or areas,

(2) Notifying internal and external organizations associated with the system,

(3) Obtaining office supplies and work space,

(4) Obtaining and installing hardware,

(5) Obtaining backup media,

(6) Restoring operating and application software,

(7) Restoring system and application data,

(8) Testing system functionality and security,

(9) Notification to user(s), and

(10) 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.

TMR-7-3, Operating Unit Contingency Planning Policies and Procedures

The Senior DOE Management PCSP is to direct operating units to develop, document, and implement contingency planning policies and procedures compliant with the requirements defined in the PCSP and commensurate with the level of security required for the organization's environment and specific needs.