National Nuclear Security Administration

NNSA Policy Letter: NAP-14.12
Date: April 5, 2006

TITLE: NNSA Contingency Planning and Operations

1. INTRODUCTION. The National Nuclear Security Administration (NNSA) possesses numerous information resources, whose exploitation or destruction by human, natural, or environmental causes could cause catastrophic health effects or casualties, could affect national prestige and morale, or affect the ability of the NNSA to perform its mission. It is not possible to protect or eliminate all vulnerabilities of all information systems, including any Critical Infrastructure or Key Resources, throughout the NNSA; however strategic improvements in security can lessen the impact of these events. In addition to strategic security enhancements, tactical security improvements can be rapidly implemented to deter, mitigate, or neutralize potential impacts. Information systems are vital elements in NNSA operations and business processes. Because these systems are essential to NNSA successfully and efficiently accomplishing its mission, the services provided by these systems must be able to operate without excessive interruption. Contingency planning supports this requirement by establishing 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 Post-Accreditation Phase of a system's lifecycle, contingency measures should be identified and integrated at all phases of the system lifecycle. This approach reduces overall contingency planning costs, enhances contingency capabilities, and reduces impacts to system operations when the contingency plan is activated.

   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 non-automated (manual) means.

2. OBJECTIVES.

   a. To implement National Institute of Standards and Technology Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, in the NNSA and all organizations under its cognizance.

   b. To establish an NNSA process for implementation of contingency planning for all NNSA major applications and general support systems.

   c. To establish requirements and assign responsibilities within the NNSA for information systems contingency planning and execution.

3. CANCELLATIONS. None.

4. APPLICABILITY. This NNSA Policy (NAP) applies to all entities, Federal or contractor, that collect, create, process, transmit, store, and disseminate information for the NNSA.

   a. NNSA Elements. NNSA Headquarters Organizations, Service Center, Site Offices, NNSA contractors, and subcontractors are, hereafter, referred to as NNSA elements or sites.

   b. Information System. This NAP applies to any information system that collects, creates, processes, transmits, stores, and disseminates unclassified or classified NNSA information. This NAP applies to any information system lifecycle, including the development of new information systems, the incorporation of information systems into an infrastructure, the incorporation of information systems outside the infrastructure, the development of prototype information systems, the reconfiguration or upgrade of existing systems, and legacy systems. In this document, the terms "information system," "cyber system," "Target of Evaluation (TOE)," or "system" are used to mean any information system or network that is used to collect, create, process, transmit, store, or disseminate data owned by, for, or on behalf of NNSA or DOE.

   c. Exclusion. The Deputy Administrator for Naval Reactors shall, in accordance with the responsibilities and authorities assigned by Executive Order 12344 (set forth in Public Law 106-65 of October 5, 1999 [50 U.S.C. 2406]) and to ensure consistency throughout the joint Navy and DOE Organization of the Naval Reactors Propulsion Program, implement and oversee all requirements and practices pertaining to this Order for activities under the Deputy Administrators cognizance.

   d. Implementation. A plan for the implementation of this NAP must be completed within 60 days after modification of the site's contract to include this NAP. A plan for the implementation of this NAP within an NNSA Federal organization must be completed within 60 days after issuance of this NAP.

5. REQUIREMENTS.

   a. Accomplish planning and documentation for contingencies, as described in Appendix 1 of Attachment 1, for each NNSA information system beginning in the Definition Phase of the Information System Certification and Accreditation Process (ISCAP), as described in NAP 14.1-A, *NNSA Cyber Security Program.*

   b. Contingency Plans for all NNSA information systems shall be implemented and tested, and results of tests documented as described in Appendix 1 of Attachment 1.

   c. The availability of information systems shall be accomplished within the time frames designated in Appendix 1 of Attachment 1.

6. RESPONSIBILITIES.

   a. The NNSA Chief Information Officer shall

      (1) Ensure the establishment of criteria for identifying information systems that provide support to, or are, Critical Infrastructure or Key Resources and

      (2) Ensure that NNSA information systems and contingency operations meet the mission and national needs through reviewing reports of Contingency Plan testing.

   b. The Service Center Manager shall

      (1) Appoint the Service Center Contingency Planning Coordinator,

      (2) Ensure the development, distribution to management staff, and enforcement of Service Center Policy for contingency planning, and

      (3) Ensure resources are available to implement contingency plans and testing for all systems under his/her purview as described in Appendix 1 of Attachment 1.

   c. The Site Office Manager shall, as described in Appendix 1 of Attachment 1,

      (1) Appoint the Site Office Contingency Planning Coordinator,

      (2) Ensure the development, distribution to management staff, and enforcement of Site Policy for contingency planning, and

      (3) Ensure resources are available to implement contingency plans and testing for the all systems under his/her purview as described in Appendix 1 of Attachment 1.

d. The Service Center Director shall, as described in Appendix 1 of Attachment 1,

(1) Appoint the Service Center Contingency Planning Coordinator,

(2) Ensure the development, distribution to management staff, and enforcement of Service Center Policy for contingency planning, and

(3) Ensure resources are available to implement contingency plans and testing for the all systems under his/her purview as described in Appendix 1 of Attachment 1.

e. Contingency Planning Coordinator

(1) Manages development, testing, test reporting, and execution of Contingency Plans.

(2) Provides testing reports of Critical Infrastructure and key Resource systems to the Office of the NNSA CIO through the Site Office.

(3) Provides testing reports of site systems that are critical to maintaining the safety and health of employees and the public and maintaining commitments to external organizations to the Site Office Manager or Service Center Director, as applicable.

(4) Ensures that contingency planning for all information systems has been accomplished.

(5) Prepare Plans of Action and Milestones for systems where current resources are lacking.

(6) Ensures the contingency plan(s) are reviewed at least annually.

(7) Ensures the contingency plan(s) for Critical Infrastructure and Key Resources systems are tested, at least annually.

(8) Conducts the Business Impact Analysis (BIA).

(9) Coordinates contingency planning with Emergency Management and Disaster Recovery planners.

(10) Coordinates with external organizations and system Points-of-Contact to ensure that impacts caused by changes within either organization will be reflected in the contingency plan.

(11) Communicate changes in contingency plans to Emergency Management and Disaster Recovery planners as necessary.

(12) Designate appropriate teams to implement the contingency strategy(ies).

(13) Determines when a contingency plan is activated.

(14) Determines the recovery strategy in coordination with users and the System Owner.

f. Application Owners/Data Owners/Data Stewards shall

(1) Ensure that applications and/or data supporting Critical Infrastructure or Key Resources are identified and

(2) Provide resources to support the implementation and testing of contingency plans for the application and data.

g. Enterprise System/ Major Application Manager shall ensure that

(1) Enterprise Systems/Major Applications and data supporting Critical Infrastructure or Key Resources are identified and

(2) Provide resources to support the implementation and testing of contingency plans for Enterprise Systems/ Major Applications.

h. Information System Owner shall

(1) Act as the Point-of-Contact for coordinating contingency requirements of all applications hosted by the system,

(2) Ensure the resources for implementation of contingency plans for their systems are identified, and

(3) Test and prepare test reports on the Contingency Plan for his/her information system.

7. CONTACT. Questions concerning this NAP should be directed to the NNSA Cyber Security Program Manager, through the Cyber Security Office Manager, at 301-903-2425.

8. DEFINITIONS. See Attachment 2.

BY ORDER OF THE ADMINISTRATOR:

Linton Brooks

Administrator

Attachments

This page intentionally blank.

ATTACHMENT 1

CONTRACTORS REQUIREMENTS DOCUMENT (CRD)

This Contractor Requirements Document establishes the requirements for National Nuclear Security Administration (NNSA) contractors and their employees. Regardless of the performer of the work, the contractor is responsible for compliance with the provisions and requirements of this CRD. The contractor is responsible for the flow down of these provisions and requirements to subcontracts at any tier to ensure the contractor's compliance with these provisions and requirements. The contractor will ensure that it and its subcontractors comply with the provisions and requirements of this CRD.

1. INTRODUCTION. Information systems are vital elements in NNSA operations and business processes. Because these systems are essential to NNSA successfully accomplishing its mission, the services provided by these systems must be able to operate without excessive interruption. Contingency planning supports this requirement by establishing 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 Post-Accreditation Phase of a systems lifecycle, contingency measures should be identified and integrated at all phases of the system lifecycle. This approach reduces overall contingency planning costs, enhances contingency capabilities, and reduces impacts to system operations when the contingency plan is activated.

   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 non-automated (manual) means.

   The contractor must systematically integrate contingency planning into management and work practices at all levels of the contractor's organization so that missions are accomplished while appropriately protecting all information on information systems and assign responsibilities for contingency planning for the purpose of ensuring the continuity of NNSA operations.

2. APPLICABILITY. This CRD applies to all contractors or sub-contractors that collect, create, process, transmit, store, or disseminate information for the NNSA.

3. IMPLEMENTATION. A plan for the implementation of this CRD must be completed within 60 days after incorporation of this CRD into the contract.

4. REQUIREMENTS.

   a. The contractor shall accomplish planning and documentation for contingencies, as described in Appendix 1, for each NNSA information system during the Information System Certification and Accreditation Process (ISCAP), as described in Attachment 1 to NAP 14.1-A, *NNSA Cyber Security Program*.

   b. The contractor shall implement, test, and prepare test reports on contingency plans for all NNSA information systems as described in Appendix 1.

   c. The contractor shall ensure the availability of information systems within the time frames designated in Appendix 1.

5. RESPONSIBILITIES.

   a. Laboratory Director or Production Facility Manager shall

      (1) Appoint the Laboratory/Production Facility Contingency Planning Coordinator,

      (2) Ensure the development, distribution to management staff, and enforcement of Site Policy for contingency planning, and

      (3) Ensure resources are available to implement contingency plans and testing for the designated systems under his/her purview.

   b. Contingency Planning Coordinator shall

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

      (2) Provide Contingency Plan test reports for Critical Infrastructure systems to the Office of the NNSA CIO through the Site Office Manager or Service Center Director, as applicable.

      (3) Provide Contingency Plan test reports for Key Resources to the Site Office Manager or Service Center Director, as applicable, through the Lab Director or production Facility Manager.

      (4) Ensure that contingency planning for all information systems has been accomplished.

      (5) Prepare Plans of Action and Milestones for systems where current resources are lacking.

(6) Ensure the contingency plan(s) are reviewed at least annually.

(7) Ensures the contingency plan(s) for Critical Infrastructure and Key Resources systems are tested, at least annually.

(8) Conduct the Business Impact Analysis (BIA).

(9) Coordinate contingency planning with Emergency Management and Disaster Recovery planners.

(10) Coordinate with external organizations and system Points-of-Contact to ensure that impacts caused by changes within either organization will be reflected in the contingency plan.

(11) Communicate changes in contingency plans to Emergency Management and Disaster Recovery planners as necessary.

(12) Designate appropriate teams to implement the contingency strategy(ies).

(13) Determine when a contingency plan is activated.

(14) Determine the recovery strategy in coordination with users and the System Owner.

c. Application Owners/Data Owners/Data Stewards shall

(1) Ensure that applications and/or data supporting Critical Infrastructure or Key Resources are identified and

(2) Provide resources are to support the implementation and testing of contingency plans for the application and data.

d. Enterprise System/Major Application Manager shall:

(1) Ensure that Enterprise Systems/Major Applications and data supporting Critical Infrastructure or Key Resources are identified and

(2) Provide resources to support the implementation and testing of contingency plans for Enterprise Systems/ Major Applications.

e. Information System Owner shall:

(1) Acts as the Point-of-Contact for coordinating contingency requirements of all applications hosted by the system,

(2) Ensure the resources for implementation of Contingency Plans for their systems are identified, and

(3) Test and prepare test reports on the Contingency Plan for his/her information system.

APPENDIX 1

PREPARING FOR CONTINGENCIES

1. INTRODUCTION. Information systems are essential to NNSA mission success; therefore, it is critical that the services provided by these systems be able to operate effectively without excessive interruption. 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 either restoring operations at an alternate location, using alternate equipment, or reverting to a manual process. Contingency planning for information systems is an integral part, but not the primary focus, of site planning for Continuity of Operations, Business Continuity, Business Recovery, Disaster Recovery, or Occupant Emergency.

2. CONTINGENCY PLANNING. The NNSA Contingency Planning Process consists of six progressive steps that are to be accomplished during the NNSA Information System Certification and Accreditation Process (ISCAP). The following planning steps lead to a contingency plan that contains detailed guidance and procedures for restoring a damaged system.

   a. Site Policy. The site's contingency planning policy statement must define the site's overall contingency objectives, establish the framework, define contingency planning responsibilities, and the criteria (safety of personnel; extent of damage to the site, facility, or system; criticality of the system to the site's mission, and anticipated disruption; etc.) for activating the contingency plan(s). The major elements to be covered in the statement are roles and responsibilities, resource requirements, training requirements, exercise and test schedules, plan maintenance schedule, frequency of backups, storage of backup media, and compliance with NNSA policy.

   b. Business Impact Analyses (BIAs) (ISCAP Definition Phase). The site shall conduct BIAs to identify systems providing services critical to site operations and prioritize these systems and their components. These BIAs are to provide sufficient information to enable the Contingency Plan Coordinator to fully characterize the system requirements, processes, and interdependencies to determine contingency requirements and priorities. The purposes of the BIA are to correlate specific systems and components with the critical services that they provide and, based on that information, to characterize the consequences of a disruption to the system components.

      (1) BIA for any system designated a Critical Infrastructure or Key Resource may be limited to a determination of critical components needed to maintain essential operation of these systems.

(2) BIAs for the remaining systems under the purview of the site must include all elements of the BIA.

(3) Identify critical information system resources.

(a) Identify data users, providers, and flows

(b) Identify the system components and infrastructure (electric power, servers, routers, authentication servers, etc) required to extract or enter data.

(4) Identify disruption impacts and allowable outage times.

(a) Identify the magnitude of expected disruptions from site-level plans, such as Disaster Recovery, Continuity of Operations, and Occupant Emergency Plans, to determine the threats from natural, human, or environmental sources.

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

(c) Identify any related or dependent systems and processes that will be disrupted by the unavailability of the system.

(d) Identify the point in time where the cost of system inoperability and the cost of restoration are equal.

(5) Develop recovery priorities.

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

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

(c) Initiate the preparation of Plans of Action and Milestones (POAMs) for any systems that are prioritized below current funding capabilities.

c. Preventive Controls (ISCAP Definition Phase). Identify measures taken or to be taken to reduce the effects of system disruptions.

(1) Identify the vulnerabilities to natural, human, or environmental threats.

(2) Develop mitigation strategies to reduce or eliminate impacts to system components, in priority order, based on the BIAs.

(3) Update Plans of Action and Milestones (POAMs) for any system that is prioritized below current funding capabilities.

d. Recovery Strategies (ISCAP Definition Phase). Develop thorough recovery strategies to ensure that the system may be recovered as effectively and as quickly as needed following a disruption.

(1) Identify the threats and/or vulnerabilities that could not be mitigated.

(2) Develop recovery strategies, such as Alternate Sites, Hot Sites, Mirrored Sites, rapid equipment replacement, and/or reallocation of existing site equipment based on the disruption impacts and the allowable outage times from the BIAs.

(3) Different types of contingency situations will necessitate different readily available staff with particular skills. The plan should identify those personnel or teams to accomplish the decision making, coordination, administrative, and technical functions required for contingency plan execution such as:

(a) Senior Management Official

(b) Management

(c) Damage Assessment

(d) Alternate Site Recovery Coordination

(e) Hardware Salvage

(f) Data Recovery

(g) Database Recovery

(h) Application Recovery

(i) LAN/WAN Recovery

(j) Telecommunications

(k) Network Operations Recovery

(l) Software and Data Recovery

(m) System Software

(n) Operating System Administration

(o) System Recovery

(p) Server Recovery

(q) Administrative Support

(r) Original Site Restoration/Salvage Coordination

(s) Test

(t) Procurement (equipment and supplies)

(u) Physical/Personnel Security

(v) Transportation and Relocation

(w) Media Relations

(x) Legal Affairs

(4) Update the POAM to include resource requirements to implement this portion of the Contingency Plan.

e. Testing, training, and exercises (ISCAP Validation Phases). Testing the plan identifies planning gaps and exercises identify planning and implementation gaps whereas training prepares recovery personnel for plan activation. These activities improve plan effectiveness and overall site preparedness.

(1) Testing – Testing a contingency plan involves the definition of a scenario, test objectives, and criteria that must be met to successfully complete the test of each Contingency Plan element.

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

(b) Test reports for Critical Infrastructure must be forwarded to the Office of the NNSA CIO through the Site Office Manager or Service Center Director, as applicable, and Key Resources forwarded to the Site Office Manager or Service Center Director, as applicable.

(c) Testing may take two forms.

i. Tabletop Exercise – This takes place in a classroom-type environment and emulates particular recovery scenarios. During plan development, tabletop exercises are conducted on portions of the plan to detect and correct initial errors and misconceptions. Tabletop exercises also provide familiarity for recovery personnel throughout the lifecycle of the system. A Tabletop Exercise of all contingency plans must be conducted annually.

ii. Functional Exercise – This takes place in a simulated environment and utilizes physical testing of procedures, alternate equipment, alternate locations, etc to ensure the correctness of procedures,

capability of recovery personnel, and technical capabilities of equipment. 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.

(2) Training – Recovery personnel must be trained to understand the contingency plan and their role in it. This training will be accomplished annually and as part of changes to the contingency plan. The following plan elements shall be included in training:

(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

(3) POAM Update – Update the POAM to include resource requirements to implement this portion of the Contingency Plan.

f. Plan maintenance (Post Accreditation Phase). 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 NNSA 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.

3. CONTINGENCY PLAN DEVELOPMENT. The plan contains detailed roles, responsibilities, teams, and procedures associated with restoring an IT system following a disruption. The contingency plan should document technical capabilities designed to support contingency operations. The contingency plan should be tailored to the site and its requirements. A site-level Contingency Plan may be written to describe processes that are common to all Contingency Plans with system-specific detail as addendums or separate contingency plans; however, plans should provide quick and clear directions in the event that personnel unfamiliar with the plan or the systems are called on to perform recovery operations. Plans should be clear, concise, and easy to implement in an emergency. Where possible, checklists and step-by-step procedures should be used. The following sections are not intended to be a required

format but to ensure sufficient information is included in the contingency plan and provide an example of how a plan may be constructed.

a. 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.

(1) Purpose. This subsection establishes the reason for writing the plan.

(2) 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.

b. 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.

(1) References/Requirements. This subsection identifies the NNSA, Program, and Site requirements for contingency planning.

(2) Record of Changes. This subsection describes the configuration history of the contingency plan by recording dates, version, and reason for contingency plan changes.

c. Concept of Operations. The Concept of Operations element provides additional detail about the system, planning framework, response activities, recovery activities, and resumption activities.

(1) 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.

(2) Line of Succession. The order of succession identifies the personnel responsible for assuming authority in the event the designated person is unavailable.

(3) Responsibilities. This subsection describes the overall structure of the contingency teams (See Section 2.c.(3)). The coordination mechanisms and requirements as well as an overview of team member roles and responsibilities are described.

d. 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.

(1) Notification Procedures. 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. Personnel to be notified may be listed in an appendix that identifies the person, their team position, home address, phone number, pager number, cell phone number, and personal and business e-mail address. Notifications to interconnected systems staff, internal or external to the site, would also be made. These points –of contact are identified in the SSP Memorandum of Agreement/System Interconnect Agreement but should also be listed in the contingency plan for ease of use when needed.

(2) 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:

(a) The cause of the emergency or disruption,

(b) The potential for additional disruptions or damage,

(c) Area affected by the emergency,

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

(e) Inventory and functional status of system components,

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

(g) System components to be replaced, and

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

(3) 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 covers personnel safety,

extent of damage to the facility, extent of damage to the system, criticality to the site's mission, and anticipated duration of disruption.

e. 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.

(1) 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.

(2) 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:

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

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

(c) Obtaining office supplies and work space,

(d) Obtaining and installing hardware,

(e) Obtaining backup media,

(f) Restoring operating and application software,

(g) Restoring system and application data,

(h) Testing system functionality and security,

(i) Notification to user(s), and

(j) Operating alternate equipment.

f. 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:

(1) Ensuring adequate infrastructure support, such as electric power, water, telecommunications, security, environmental controls, office equipment, and supplies;

(2) Installing system hardware, software, and firmware. This activity should include detailed restoration procedures similar to those followed in Recovery;

(3) Establishing connectivity and interfaces with network components and external systems;

(4) Testing system operations and security to ensure full functionality;

(5) Backing up operational data on the contingency system and uploading to restored system;

(6) Shutting down the contingency system;

(7) Terminating contingency operations;

(8) Securing, removing, and/or relocating all sensitive materials at the contingency site; and

(9) Arranging for recovery personnel to return to the original facility.

4. Contingency Plan Structure. The structure of a contingency plan is based on the importance of systems for which the plan is written. The following sections describe the mandatory contingency plan elements based on the designation of the system.

a. 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 system in a different location.

b. 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 system in a different location.

(1) Introduction (Paragraph 3.a)

(2) Scope (3.b.)

(3) Concept of Operations (3.c.)

(4) Notification/Activation (3.d.)

(5) Recovery Procedures (3.e.(2))

(6) Reconstitution (3.f.)

c. Remaining Systems. All other system contingency plans must address each of the elements as indicated in the sections below in sufficient detail for personnel who normally operate the systems to restore operations.

(1) Introduction (3.a)

(2) Scope (3.b)

(3) Concept of Operations

(a) System Description (3.c.(1))

(b) Line of Succession (3.c.(3))

(4) Notification/Activation

(a) Notification Procedures (3.d.(1))

(b) Plan Activation (3.d.(3))

(5) Recovery Procedures

(a) Hardware Installation (3.e.(2)(d))

(b) Backup Media (3.e.(2)(e))

(c) Software Restoration (3.e.(2)(f))

(d) Functional and Security Testing (3.e.(2)(h))

(e) User Notification (3.e.(2)(i))

(6) Reconstitution

(a) Infrastructure Support (3.f.(1))

(b) Internal and External Networking (3.f.(3))

(c) Functional and Security Testing (3.f.(4))

ATTACHMENT 2

DEFINITIONS

The following are terms and definitions used in this NAP that are not found in National Security Telecommunications and Information Systems Security Committee (NSTISSC) 4009, National Information Systems Security (INFOSEC) Glossary, dated 5 June 1992. The NSTISSC has been renamed The Committee on National Security Systems.

Computing Environment	The total environment in which an automated information system, network, or a component operates. The environment includes physical, administrative, and personnel procedures as well as a communication and networking relationship with other information systems.
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 Owner	The person responsible for having information reviewed for sensitivity and classification. This person is responsible for its generation, management, and destruction.
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.
Information System	The infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. Any telecommunication or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware. [Office of Management and Budget, Circular A-130, Nov 30, 2000: A discrete set of information resources organized for the collection, processing, maintenance, transmission, and

	dissemination of information in accordance with defined procedures, whether automated or manual.]
Information System Certification and Accreditation Process (ISCAP)	
	The standard NNSA process for identifying information security requirements, providing security solutions, managing information system security activities, and authorizing the operation of a system.
Key Resources	Publicly or privately controlled resources essential to the minimal operations of the economy and government.
Major Application	A major application is an application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. [From Appendix III, OMB A-130]
	An application that requires special management attention to provide security over and above the GSS on which it resides because of its importance to an organizations' mission; its high development, operating, or maintenance costs; or its significant role in the administration of an organization's programs, finances, property, or other resources. Site management determines organizational scope and the definition of "significant".
Mission	The assigned duties to be performed by an information system.
Site	An NNSA facility: can be a NNSA Service Center, NNSA Site Office, NNSA contractor or subcontractor facility, or the NNSA Headquarters activity that has a responsibility to protect NNSA information systems. It has a set of geographical boundaries as defined in a NNSA SSSP or SSP.

Site Manager	The person responsible for management of all activities at a site.
System	The set of interrelated components consisting of mission, environment, and architecture as a whole.
System Owner	The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system. The system owner, based on previous information, also has some security duties.