NNSA POLICY LETTER

NAP 14.1-C

Approved: 05-02-08

NNSA BASELINE CYBER SECURITY PROGRAM

NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of the Chief Information Officer

AVAILABLE ONLINE AT:
http://hq.na.gov

INITIATED BY:
Office of the Chief Information Officer

This page intentionally left blank.

Table of Contents

Appendices

Figures

Tables

NNSA BASELINE CYBER SECURITY PROGRAM

OVERVIEW

1. PURPOSE.

   a. Implement DOE O 205.1A, *Department of Energy Cyber Security Management*, and TMR-0, DOE *Cyber Security Program Foundation* in the National Nuclear Security Administration (NNSA) and all Elements under its cognizance.

   b. Establish an NNSA Program Cyber Security Plan (PCSP) that systematically integrates cyber security into management and work practices at all levels in the NNSA so that missions are accomplished while appropriately protecting all information on information systems.

   c. Establish requirements and assign responsibilities within the NNSA PCSP for protecting information on information systems.

   d. Ensure the NNSA PCSP is consistent with, and achieves the objectives of Executive Orders, National Security Directives, DOE Orders and Manuals, and Federal regulations.

   e. Establish a NNSA cyber security process that addresses program requirements, defines protection measures, provides cyber security planning, and implements the NNSA PCSP.

   f. Implement requirements in Public Law (PUB.L.) 100-235 (1987), the Federal Information Security Management Act of 2002 (FISMA), Presidential Directives and Executive Orders, Office of Management and Budget (OMB) directives, National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS), Departmental policies, and the DOE CIO Cyber Security Technical and Management Requirements (TMRs).

2. CANCELLATIONS. This NNSA Policy replaces NNSA Policy Letters (NAPs) 14.1-B, 14.2-B, 14.3-A, 14.4-A, 14.5-A, 14.6-A, 14.7A, 14.8A, 14.9A, 14.10A. 14.11-A, 14.12, 14.13, 14.14, 14.15, and 14.16.

3. APPLICABILITY. This NAP applies to all NNSA entities, Federal or contractors, that collect, create, process, transmit, store, and disseminate information on automated information systems for the NNSA.

   NNSA Elements. NNSA Headquarters (HQ) Site, Organizations, Service Centers, Site Offices, NNSA contractors, and subcontractors are hereafter referred to as NNSA Elements or sites. This NAP applies to all NNSA Elements.

   a. 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 term(s) "information system," "cyber system," or "system," are used to define any information system or network used to collect, create, process, transmit, store, or disseminate data owned by, for, or on behalf of, NNSA or DOE.

b. Exclusions.

(1) 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.

(2) The NNSA PCSP does not apply to Sensitive Compartmented Information (SCI) information systems located at NNSA sites. SCI systems must comply with Director, Central Intelligence Directives (DCIDs), or Intelligence Community Directives (ICDs) security policies. The DOE Office of Intelligence and Counterintelligence approves operation of these information systems.

(3) 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 implementation of this NAP within an NNSA Federal organization must be completed within 60 days after issuance of this NAP. The implementation plan must include, at a minimum, the program activity to be modified and created; the starting date of revision or development; the estimated due date; and the responsible party for the stated activity. This implementation plan shall not exceed three years from the date of formal approval of the implementation plan. The implementation plan must be approved by the local NNSA Designating Approval Authority (DAA). This means that the NNSA Element's Cyber Security Program (CSP) must comply with all requirements set forth in this NAP. Further, all information systems as defined in the Glossary must be protected in accordance with the requirements set forth in this NAP.

4. BACKGROUND. The loss or compromise of information entrusted to NNSA or its contractors may affect the National Security, the Nation's economic competitive position, the environment, NNSA missions, and other citizens of the United States. All

information collected, created, processed, transmitted, stored, or disseminated by, or on behalf of, the NNSA on automated information systems requires some level of protection. Loss or compromise of information entrusted to NNSA or its contractors may affect the nation's economic competitive position, the environment, the National Security, NNSA missions, or the citizens of the United States. The risk management approach defined in the NNSA CSP provides for the graded, cost-effective protection of information systems containing unclassified or classified information.

The NNSA NAP 14 series, NNSA Threat Statement, the NNSA Risk Assessment document, and the NNSA CSP comprises the NNSA PCSP. The NNSA PCSP systematically integrates cyber security into management and work practices at all levels in the NNSA so that missions are accomplished while appropriately protecting all information on information systems; establishes requirements and responsibilities for protecting information on information systems for the purpose of maintaining National Security and ensuring the continuity of NNSA operations; and ensures that NNSA cyber security is consistent with, and achieves the objectives of all applicable Executive Orders, National Security Directives, DOE Orders and Manuals, and Federal regulations.

a. The PCSP is implemented through a CSPP for each NNSA Element.

b. Risk management is a process that considers the prevailing NNSA threat analysis, the attributes of the information being protected, the effect of countermeasures in place and planned, and the remaining vulnerability of the processing environment (residual risk).

c. The PCSP establishes minimum protection requirements based on the Consequences of Loss (CoL) of confidentiality, integrity, and availability of all information.

d. Protection requirements for all information systems are documented in Information System Security Plans (ISSPs).

e. The PCSP is consistent with other NNSA Directives and DOE Orders, Manuals, and Technical and Management Requirements that provide specific security requirements for information systems, including communications systems, transmission systems, as well as classified and unclassified matter through administrative procedures, logical access, and physical security requirements.

f. The NNSA PCSP implements the following DOE cyber security policies and guidelines:

- DOE P 205.1, *Departmental Cyber Security Management Policy*
- DOE O 205.1A, *Department of Energy Cyber Security Management*
- DOE M 205.1-4, *National Security System Manual*
- DOE N 206.5, *Response and Notification Procedures for Data Breaches Involving Personally Identifiable Information*
- DOE CIO TMR-0, *DOE Cyber Security Program Foundation*
- DOE CIO TMR-4, *Vulnerability Management*

- DOE CIO TMR-6, *Plan of Action and Milestones*
- DOE CIO TMR-8, *Configuration Management*
- DOE CIO TMR-12, *Wireless Devices and Information Systems*
- DOE CIO TMR-13, *Portable and Mobile Devices*
- DOE CIO TMR-14, *External Information Systems*
- DOE CIO TMR-18, *Peer-to-Peer (P2P) Networking*

5. REQUIREMENTS. NNSA Elements must implement and manage a risk-based CSP. Risk-based approaches, procedures, and other means must be used to evaluate and verify effectiveness of cyber security measures, identify areas requiring improvement, and validate implemented improvements. The following paragraphs address these approaches and procedures.

   a. Protection Measures. Protection measures for all NNSA information systems must conform to the protection measures described in the NNSA PCSP, the NNSA Element's CSPP, and the ISSP.

      (1) Protection measures may be strengthened based on an assessment of unique local threat(s) or the local evaluation of CoL.

      (2) All Governmental information and any non-Governmental information on an NNSA information system must be considered when determining the system's protection measures.

   b. Information Groups. An NNSA Information Group contains all information that requires similar protection or is similar in content, use, or sensitivity. All NNSA information must be identified as part of an NNSA-approved Information Group. Chapter V contains the definition of NNSA Information Groups and the mapping between the Information Groups and DOE cyber security enclave classes. Chapter XVII further details what information is considered to be Sensitive Unclassified Information (SUI), including Personally Identifiable Information (PII).

   c. Classified Information Access. Access to classified information must be granted only to persons with the appropriate access authorization and Need-to-Know in the performance of their duties according to NNSA policies and DOE M 470.4-4, *Information Security*. The individual disseminating the information is responsible for determining the recipient's Need-to-Know in accordance with the site's processes and NNSA policies and guidance.

   d. Unclassified Information Access. Access to unclassified information must be granted to only those persons who have the appropriate access authorization and Need-to-Know for the information in the performance of their duties. The individual disseminating the information is responsible for determining the recipient's Need-to-Know in accordance with the site's processes and NNSA

policies and guidance.

e. Knowledge and Resources. All NNSA Element personnel must possess the knowledge, skills, equipment, and resources to fulfill their cyber security responsibilities under both normal and emergency conditions. The primary roles and responsibilities of all applicable NNSA Element personnel are described in Chapter II.

f. Facility Clearance and Registration. NNSA Elements with classified information systems must obtain prior approval access through the Facility Clearance and Registration Process, as outlined in DOE M 470.4-1, *Safeguards and Security Program Planning and Management.*

g. Risk Management Process. The NNSA Element must implement the risk management process and requirements described in Appendix H.

h. Configuration Management. The NNSA Element must implement NNSA Configuration Management (CM) policies and processes for all NNSA information systems within the Element, as described in Chapter III.

i. Cyber Security Program Plan (CSPP). The NNSA Element must implement the CSPP processes and requirements described in Chapter IV.

j. Deviations. Any deviation from the NNSA cyber security requirements and pr Serves as the DAA for all information systems whose perimeter or presence as described in an ISSP is wholly contained (Federal or contractor) under the cognizance of the NNSA Service Center. The Service Center Director/Manager's DAA approval authority may be delegated to another Federal employee of the Service Center, or through a memorandum of agreement, to NNSA Federal employees at the NNSA Headquarters Site or a Site Office. Processes must be documented and approved, as described in Chapter VI.

k. Incident Management. NNSA Elements must implement established requirements and responsibilities for cyber security incident preparation, prevention, warnings, reporting, and recovery from cyber security incidents involving NNSA information systems.

l. INFOCON. NNSA Elements must implement established requirements and guidance for standardized procedures and responsibilities for authorizing and communicating Information Conditions (INFOCONs) within the Element, and to or from the NNSA Office of the Chief Information Officer (OCIO).

m. Plan of Actions and Milestones (POA&M). NNSA Elements must implement established requirements for tracking and mitigation of CSP and system-level weaknesses identified at specific NNSA sites.

n. Vulnerability Management. NNSA Elements must implement established

requirements for the development of a vulnerability management program, to include patch management procedures, for NNSA information systems.

o. Foreign National Access. NNSA Elements must implement established requirements for allowing Foreign National Access to NNSA information systems to include, but not be limited to, computers, networks, associated servers, data storage devices, and portable or mobile devices.

p. Portable Computing Devices. NNSA Elements must implement established requirements for the use of non-Government owned or Government-owned portable computing devices for NNSA and all organizations under its cognizance.

q. Password Protection. NNSA Elements must implement established requirements for the generation, protection, and use of passwords to support authentication when accessing classified and unclassified NNSA information systems, applications, and resources.

r. Wireless, Remote, and Peer-to-Peer (P2P) Networking Technologies. NNSA Elements must establish minimum security controls as appropriate to protect NNSA information systems, applications, and software, when implementing wireless, remote, and P2P technologies.

6. DEFINITIONS. The Glossary in Appendix B defines the acronyms, abbreviations, and terms used in this document.

7. CONTACTS. Questions concerning this NAP should be directed to the Cyber Security Program Manager (CSPM), at 202-586-9728.

BY ORDER OF THE ADMINISTRATOR:

THOMAS P. D'AGOSTINO
Administrator

CHAPTER I. NNSA PCSP OVERVIEW

1. INTRODUCTION. The requirements of the NNSA PCSP, as detailed in this NAP, apply to any information system or network that is used to collect, create, process, transmit, store, or disseminate information for the NNSA. The NNSA PCSP implements National and Departmental cyber security policies.

2. PCSP MANAGEMENT. While cyber security is everybody's responsibility, there are several positions that have key roles in the NNSA PCSP. They are: 1) the CSPM; 2) the DAA; 3) the Information System Security Office Manager (ISOM); 4) the Information Systems Security Site Manager (ISSM); 5) the Information System Owner (ISO); and 6) the Information System Security Officer (ISSO). The roles and responsibilities for these positions are described in Chapter II.

3. CYBER SECURITY PROGRAM PLAN. Implementation of the NNSA PCSP is documented in a CSPP. A CSPP must be prepared for each NNSA Element, unless the Element is covered under another CSPP. The CSPP is the document that outlines the policies, procedures, and practices of an Element's CSP. The CSPP is a management-level document that details the Element's policies, procedures, and practices for ensuring effective cyber security. It also explains the site, or application-specific environment, missions, and threats. The policies, procedures, practices, environments, missions, and threats that are applicable to systems and major applications at the Enterprise level are documented in the NNSA Element's CSPPs.

4. MINIMUM INFORMATION SYSTEM SECURITY CONFIGURATIONS. The NNSA PCSP requires all NNSA Elements to implement and maintain NNSA-approved minimum security configurations. The minimum security configurations for unclassified and classified information systems, as determined by the system categorization process, are listed in NAP 14.2-C, *NNSA Certification and Accreditation (C&A) Process*, Chapter III. Each NNSA Element must implement NNSA-specified or NNSA-approved monitoring capabilities to ensure that protection features defined in the approved minimum security configurations are maintained in the system. If the minimum security configuration cannot be implemented, this must be stated in the Risk Assessment for the system. The monitoring capability must provide continuous review and reporting of the status of the minimum security configuration specified for each information system. The monitoring capability must provide the ability to continuously detect and manage changes in software used in the information system components.

   If an information system cannot implement an NNSA-approved minimum information system security configuration due to operational or mission requirements, a new minimum security configuration must be developed and approved by NNSA CSPM.

   The minimum security configuration must provides assurance that all security measures

are implemented and maintained in the information system, documented in the ISSP, and approved by the local NNSA DAA.

5. CERTIFICATION AND ACCREDITATION. The NNSA PCSP implements the National and Departmental requirements for the C&A of all information systems. The NNSA PCSP requires that each information system be accredited every three (3) years, or when significant changes have been made to the system, the system environment, the threat, or cyber security requirements, in response to changes in the NNSA PCSP. Each information system must receive an accreditation, *i.e.,* approval to operate (ATO) or an interim approval to operate (IATO), before beginning operational activities. NAP 14.2-C, *NNSA C&A Process*, sets forth the requirements for the C&A program.

6. INFORMATION SYSTEM SECURITY PLAN (ISSP). All information systems processing information at a site must be included as part of an ISSP, and they must receive an ATO or IATO before production. The ISSP is the basis for C&A process. The ISSP documents the security environment in which the information system exists, such as the cyber security requirements needed to protect the information on the system, and implementation of the cyber security requirements for formal accreditation of the information system. The ISSP must be tailored to address the characteristics of the information system, operational requirements, security policy, and prudent risk management throughout the system's lifecycle as conditions change. Required information for the ISSP is thoroughly described in NAP 14.2-C, *NNSA C&A Process*.

CHAPTER II. MANAGEMENT STRUCTURE AND RESPONSIBILITIES

1. INTRODUCTION. The NNSA PCSP is managed through a multi-tiered structure. The structure includes a CSPM, DAA, ISOM, ISSM, and an ISSO at NNSA Headquarters (HQ). ISOM(s), ISSM(s), and ISSO(s) are located at the NNSA Service Centers and NNSA Site Offices. The ISSMs and ISSOs may also be located at contractor locations. The structure also includes NNSA Enterprise Systems and Major Application Program Managers, Certification Agents (CAs), system owners, application owners, data owners, data stewards, and users of the systems. This chapter describes the roles and responsibilities of the individuals involved in the NNSA PCSP.

2. RESPONSIBILITIES.

a. Administrator, National Nuclear Security Administration:

(1) Retains ultimate accountability for cyber security and accepts the residual risk that exists within each of the NNSA Elements through the approval of the NNSA PCSP.

(2) Appoints the NNSA CSPM, who is the focal point for cyber security within the NNSA.

b. Associate Administrator for The Chief of Defense Nuclear Security: The Associate Administrator for the Chief of Defense Nuclear Security is responsible for the strategic direction and management of the cyber security program.

c. NNSA Chief Information Officer (CIO). The CIO is responsible for the NNSA CSP and for overseeing security requirements. The CIO's responsibilities include:

(1) Ensures that cyber security is integrated into all policies and procedures used to plan, procure, develop, implement and manage the NNSA infrastructure and systems.

(2) Ensures that cyber security is integrated into the NNSA Enterprise Architecture.

(3) Ensures that architectures are consistent with current and planned computing and communication assets within the NNSA Enterprise.

(4) Recommends a qualified person to the NNSA Administrator to fill the position of CSPM.

(5) Makes and disseminates to NNSA sites determinations on the INFOCON for NNSA.

d. Cyber Security Program Manager. The CSPM is responsible for managing the CSP within NNSA. The CSPM is required to spend a minimum of one week at each NNSA field location.

(1) Serves as the DAA for all classified and unclassified information systems where perimeter or presence as described in an ISSP is wholly contained within the NNSA HQ Site and within contractor or subcontractor facilities under the cognizance of the NNSA HQ Site. The DAA may be delegated to another individual who must be a Federal employee of the Office of the NNSA CIO. The DAA's authority may be assigned to other NNSA DAAs. All CSPM delegations and assignments by the CSPM must be documented in the NNSA HQ Site CSPP.

(2) Approves the NNSA HQ Site CSPP. The CSPP approval authority may be delegated to another individual who must be a Federal employee of the Office of the NNSA CIO Element.

(3) Ensures the appointment of an ISOM responsible for oversight of the implementation of the NNSA PCSP at the NNSA HQ Site, as well as at each contractor and subcontractor organization under the cognizance of NNSA HQ. Note that the ISOM and DAA for the NNSA HQ Site may be the same individual.

(4) Ensures the appointment of an ISSO for each information system at the NNSA HQ Site.

(5) Ensures the appointment of an ISSM to be responsible for developing and implementing the CSPP at the NNSA HQ Site.

(6) Ensures the appointment of an ISSM to be responsible for ensuring the development and implementation of the CSPP in each contractor and subcontractor organization under the cognizance of the NNSA HQ Site.

(7) Ensures that the NNSA PCSP is implemented at NNSA HQ Site.

(8) Ensures that all NNSA HQ Site personnel that use information systems and systems data are aware of and fulfill their duties as described in the NNSA PCSP.

(9) Approves all NNSA CSPPs from contractors and subcontractors under the cognizance of NNSA HQ.

(10) Ensures that oversight reviews of all contractor and subcontractor sites (facilities) under the cognizance of NNSA HQ are conducted in accordance with the Survey (oversight) program defined in DOE M 470.4-1. Also ensures that processes and programs allowing access to

information systems by Foreign Nationals are assessed as part of these reviews.

(11) Ensures adequate resources are allocated to the HQ Site CSP.

(12) Ensures that the effectiveness of the NNSA HQ Site CSP is monitored through self-assessments and reviews.

(13) Ensures that the NNSA HQ Site DAAs, ISSMs, ISSOs, users, and System Administrators are trained in their specific duties, and the technologies for which they have responsibilities.

(14) Ensures the implementation of the NNSA PCSP throughout NNSA.

(15) Serves as the NNSA primary point of contact (POC) for cyber security.

(16) Represents the NNSA PCSP before Federal, private, and public organizations concerned with protecting unclassified and classified Government information.

(17) Serves as the DAA for all NNSA Enterprise information systems or Major Applications and other information systems or major applications with a perimeter or presence on different or multiple sites. This DAA authority may be assigned to other NNSA DAAs. All CSPM delegations and assignments must be documented. Ensures development and coordination of corrective actions plans involving NNSA Enterprise systems in response to issues identified by other Federal agencies (e.g., Office of Independent Oversight), peer reviews, and self-assessments.

(18) Develops, coordinates, disseminates, and maintains NNSA NAPs and guidance on all aspects of the NNSA PCSP, including coordination with telecommunications security, TEMPEST, and Public Key Infrastructure (PKI) programs.

(19) Annually reviews, and updates, as necessary, the NNSA Threat Statement, NNSA Cyber Risk Assessment, NNSA PCSP, and any NNSA-approved minimum information system configuration standards.

(20) Establishes and coordinates NNSA cyber security training, education, and awareness programs.

(21) Ensures that education in NNSA cyber security policies and practices is available to NNSA DAAs, ISOMs, ISSMs, ISSOs, Certification Agents (CAs), and system administrators. Ensures that this training is presented on a semi-annual basis.

(22) Maintains an NNSA information assurance response capability. This capability maintains and coordinates NNSA cyber incident response procedures to provide timely assistance and system vulnerability information, watch and warning capabilities, analysis, and assistance reviews to all NNSA Elements.

(23) Evaluates incident reports for NNSA Computer Network Attack (CNA), and Computer Network Exploitation (CNE) situations.

(24) Recommends changes in NNSA INFOCON to the NNSA CIO.

(25) Through the most rapid means possible, notifies NNSA Elements, through the cognizant DAAs, when the NNSA INFOCON is changed.

(26) Provides copies of approved CSPPs to other organizations, as required in NNSA policies.

(27) Monitors compliance and effectiveness of the PCSP through program reviews, budget reviews, self-assessments, management assessments, performance metrics and analysis, analysis of the results of peer reviews, vulnerability analysis, and independent oversight evaluations.

(28) Coordinates with the Office of HSS, Office of Defense Nuclear Security, Nuclear Safeguards and Security Program Organization, and Office of Independent Oversight on monitoring implementation of the PCSP, through joint review of self-assessment and oversight documentation.

(29) Coordinates with the DOE Office of Intelligence and Counterintelligence on cyber security matters that affect SCI systems at NNSA facilities.

(30) Identifies NNSA cyber security resource requirements to ensure sufficient resources are planned and budgeted.

(31) Coordinates with the NNSA Office of Planning, Programming, Budgeting, and Evaluation and the Chief Financial Officer (CFO) on budgets and expenditures related to NNSA cyber security.

(32) Manages a cyber security technology development program to support the NNSA PCSP and to periodically brief NNSA Program Managers, DAAs, ISOMs, and ISSMs, on activities and results of the program.

(33) Approves secure remote diagnostic and maintenance facilities proposed for use with information systems that process classified information for the HQ Element.

(34) Manages NNSA-wide cyber security incident reporting and response activities, in coordination with the Office of HSS, DOE Office of Associate Chief Information Officer (AOCIO) for Cyber Security, Defense Nuclear Security, the Nuclear Safeguards and Security organization, Office of Intelligence and Counterintelligence, or Office of Inspector General (OIG), as circumstances warrant.

(35) Addresses differences and resolves conflicts between the NNSA program and the DOE-M 470.4-1 program.

(36) Coordinates with the Office of HSS and the DOE Office of Associate CIO for Cyber Security on cyber security policy and the NNSA PCSP.

(37) Coordinates, as needed, with DOE Office of Intelligence and Counterintelligence on:

(a) Matters relating to policy and technical planning of counterintelligence activities.

(b) Counterintelligence investigative activities.

(c) Counterintelligence inspections, including evaluation of the CSP.

(d) Counterintelligence threat information.

(e) Matters related to the cyber threat.

(38) Coordinates, as needed, with the DOE Office of the Inspector General (IG), on IG investigation activities involving NNSA information systems.

(39) Coordinates, as needed, with the DOE Office of HSS on HSS inspection activities involving NNSA information systems.

(40) Reports changes in ISOM and DAA appointments to all ISOMs and DAAs.

(41) Supports, maintains, and coordinates an advice and assistance capability for use by any DAA, ISOM, or ISSM within NNSA. This capability includes the review of information systems protection measures as requested by the Element.

(42) Approves NNSA cyber security waivers and exceptions.

(43) Approves minimum security configurations for use in all NNSA Elements.

e. Service Center Director:

(1) Assumes responsibility and accountability for the NNSA Service Center CSP.

(2) Serves as the DAA for all classified and unclassified information systems whose perimeter or presence as described in an ISSP is wholly contained (Federal or contractor) under the cognizance of the NNSA Service Center. The Service Center Director or Manager's DAA approval authority may be delegated to another Federal employee of the Service Center, or through a memorandum of agreement, to NNSA Federal employees at the NNSA HQ Site or a Site Office.

(3) Appoints in writing an ISOM responsible for oversight of the implementation of the NNSA PCSP in each NNSA Element (including the Service Center), under the cognizance of the NNSA Service Center. The DAA and ISOM responsibilities may be filled by one person.

(4) Appoints in writing an ISSM responsible for oversight of implementation of the NNSA PCSP in the Service Center and each contractor and subcontractor organization under the cognizance of the NNSA Service Center.

(5) Ensures development, implementation, and maintenance of a CSPP for the Service Center.

(6) Ensures development and implementation of the CSPP at each contractor and subcontractor site under the cognizance of the Service Center.

(7) Ensures that all Service Center personnel that use information systems and the information on the systems are aware of and fulfill their duties as described in the PCSP and the CSSP.

(8) Ensures monitoring of cyber security effectiveness through self-assessments and reviews.

(9) Ensures that adequate resources hosted within the Service Center are allocated for the conduct of the Service Center CSP and applicable Enterprise System Major Applications.

(10) Ensures that Service Center DAAs, ISOMs, ISSMs, ISSOs, users, and System Administrators are trained in their specific duties and the technologies for which they have responsibilities.

f. Site Office Manager:

(1) If the Site Office is not covered in another CSPP, ensures the development, implementation, and maintenance of a CSPP for the Site Office.

(2) Assumes responsibility and accountability for the Site Office CSPs.

g. DAA's Representative

(1) Serves as the DAA for all information systems whose perimeter or presence as described in an ISSP is wholly contained within an NNSA Site (Federal or contractor), under the cognizance of the NNSA Site Office. The Site Office Manager's DAA approval authority may be delegated to other employees of the Site Office, or through a memorandum of agreement, to Federal employees of another Site Office or the NNSA Service Center. Note that this does not apply to HQ.

(2) Under the cognizance of the NNSA Service Center, appoints in writing an ISOM responsible for oversight of implementation of the NNSA PCSP in each NNSA Element. The DAA and ISOM responsibilities may be filled by separate individuals.

(3) Ensures the appointment of an ISSM responsible for developing and implementing the CSPP in the Site Office, unless the Site Office receives cyber security services from the Service Center.

(4) Ensures the appointment of an ISSM responsible for developing and implementing the CSPP in each NNSA Element under their cognizance.

(5) Ensures each information system in the Site Office has an appointed ISSO.

(6) Ensures that all Site Office personnel that use information systems and system data are aware of and fulfill their duties.

(7) Approves all NNSA CSPPs from NNSA Elements under the cognizance of the Site Office Manager.

(8) Ensures that oversight reviews of all sites under the cognizance of the Site Office Manager are conducted in accordance with the Survey (oversight) program defined in DOE M 470.4-1. Ensures the process and program allowing access to information systems by Foreign Nationals is assessed as part of these reviews.

(9) Under the ISOM's purview, ensures adequate resources are allocated to the Site Office CSP and are applicable Enterprise System and Major Applications.

(10) Monitors effectiveness of cyber security through self-assessments and reviews.

(11) Ensures that Site Office DAAs, ISOMs, ISSMs, ISSOs, users, and System Administrators are trained in their specific duties and the technologies for which they have responsibilities.

h. Contractors. Appendix C, *Contractor Requirements Document (CRD)*, describes the responsibilities of contractors.

i. Designated Approving Authority. The DAA is a Federal employee who has the authority to grant formal accreditation to operate, withdraw accreditation, suspend operations, grant IATOs, or grant variances when circumstances warrant. The approval shall be a written, dated statement of accreditation that sets forth clearly any conditions or restrictions to system operation. The DAA is the only individual who may accept all risks for systems under their cognizance. The DAA can delegate any of the following responsibilities to a DAA Representative (Rep), except the authority to grant accreditations or IATOs**.** DAAs are responsible and accountable for the security of the information and systems that the DAA accredits**.** Responsibilities of the DAA include:

(1) Ensures that each system is properly accredited based on a) its environment and sensitivity levels, and b) a review and approval of security safeguards and the issuance of written accreditation statements.

(2) Ensures that PCSP implementation within operating units under their cognizance.

(3) Ensures that documentation is maintained for all information system accreditations under their purview.

(4) Ensures that all appropriate roles and responsibilities are accomplished as required for each information system.

(5) Ensures that operational information system security policies are promulgated for each system, project, program, and site for which the DAA has approval authority.

(6) Should the DAA choose to accredit a system that does not have all security requirements implemented due to fiscal or operational restraints, the DAA may choose to accredit the system in accordance with interim approval criteria as stated in NAP 14.2-C, NNSA C&A Process, or accept any additional risk and issue a full approval to operate for the system.

(7) Recommends approval for waivers and exceptions and forwarding such information to the CSPM as appropriate.

(8) The DAA will ensure when a security patch cannot be applied. He or she must approve the Deviations Process and provide a copy to HQ.

(9) Disseminates INFOCON status changes received from the CSPM.

(10) Approves P2P applications during the C&A process.

(11) Approves alternatives to tamper indicating devices for portable mobile devices.

(12) Approves all products or software used to perform clearing, sanitization, or destruction of storage media.

(13) Completes NNSA-sponsored DAA training within three (3) months of assuming the DAA position. The ISOM-designated Field DAA's Representative must attend a two-week assignment at NNSA HQ.

(14) Participates in an ongoing NNSA cyber security training and awareness program.

(15) Ensures that Security Testing and Evaluation (ST&E) procedures are completed and documented.

(16) Maintains appropriate system accreditation documentation.

(17) Evaluates threats and vulnerabilities to ascertain whether additional safeguards are needed.

(18) Ensures that all risks not mitigated are documented for DAA acceptance, and the Plans of Actions and Milestones (POA&M) are created, if applicable.

(19) Ensures that a record of all security-related vulnerabilities and incidents is maintained.

(20) Ensures that certification is accomplished for each NNSA information system, network, and application under their responsibility.

(21) Evaluates certification documentation as required during C&A activities.

(22) Ensures that all ISSMs and ISSOs receive technical and security education and training to carry out their duties.

(23) Assesses changes in a system, its environment, and operational needs that could affect the accreditation.

(24) Oversees and reviews periodically system security to accommodate possible changes that may have taken place.

(25) Approves incident reporting procedures developed by the ISSM.

(26) Determines the Levels of Concern (LOC) for confidentiality, integrity, and availability for the data on a system.

(27) Ensures consideration and acknowledgement of counterintelligence activities during the C&A process.

(28) Approves system disposal plans and procedures.

j. Information System Security Officer Manager (ISOM). The ISOM is a Federal employee responsible for ensuring that operational security is maintained for information systems under the DAA's cognizance throughout the life cycle of the systems. The ISOM is also responsible for coordinating security-related incident communications between the site, the Information Assurance Response Center (IARC), and NNSA HQ. The ISOM must have a working knowledge of system functions, cyber security policies, and cyber security protection measures. If an ISOM is not appointed, the DAA assumes the ISOM responsibilities, which may be delegated to a DAA Rep. Responsibilities of the ISOM include:

(1) Evaluates security plans and ensures systems are operated, maintained, and disposed of in accordance with internal security policies and practices outlined in the ISSP.

(2) Reports all security-related incidents to the IARC and DAA.

(3) Initiates protective or corrective measures when a security incident or vulnerability is discovered.

(4) Provides monthly incident status reports to the DAA and IARC.

(5) Follows procedures approved by the DAA for authorizing software, hardware, and firmware use before implementation on the system.

(6) Conducts periodic reviews to ensure compliance with the CSPP and ISSPs.

k. Information Systems Security Site Manager (ISSM). The ISSM is a Federal employee appointed by the NNSA Element manager to be responsible for development of the Element's CSPP and implementation of the Element's CSP. The ISSM must have a working knowledge of system functions, cyber security policies, and cyber security protection measures. Any of the following duties may be delegated to an Alternate or Assistant ISSM.

(1) Maintains record copies of the Element's CSPP and ensures that the record copy of each ISSP is maintained for systems under their cognizance.

(2) Ensures appointments in writing of ISSOs for information systems operated by the NNSA Element and ensures that each ISSO and System Administrator is aware of and fulfills their cyber security duties as described in the PCSP and the Element's CSPP. ISSOs are responsible to the ISSM for fulfilling their duties.

(3) Ensures the development, documentation, and presentation of information systems security education, awareness, and training activities for Element management, cyber security personnel, application owners, data stewards, and users.

(4) Ensures that users are trained on the information system cyber security features, operation, and safeguards prior to being allowed access to the system.

(5) Ensures that training is available for ISSOs and System Administrators for information systems, cyber security requirements, operations, safeguards, Information Condition (INFOCON), and incident handling procedures.

(6) Establishes, documents, and monitors the Element's CSP implementation and ensures Element compliance with the NNSA PCSP. Upon completion of each assessment or review, the ISSM must ensure that a corrective action plan (CAP) is prepared and implemented for all findings or vulnerabilities.

(7) Identifies and documents, in coordination with the organization's Operations Security (OPSEC) program and Counterintelligence programs, Element-specific threats to information systems, and information at the site.

(8) Develops and documents additional or modified protection measures for those threats and identifies any site-wide protection measures and practices that apply to all site systems.

(9) Obtains approvals for modified protection measures from the DAA.

(10) Ensures that the CSPP is coordinated with other site plans and programs to include: Disaster Recovery; Site Safeguards and Security Plan (SSSP) or Site Security Plan; Classified Matter Protection and Control; Physical Security; Personnel Security; Telecommunications Security; TEMPEST; Technical Surveillance Countermeasures; Operations Security; and Nuclear Materials Control and Accountability.

(11) Ensures development of procedures to implement the Element's CSP on all information systems.

(12) If appointed as the CA, certifies to the cognizant DAA that the protection requirements described in the C&A Package for each information system have been implemented and are operational.

(13) Ensures that the cognizant DAA is notified when the information system is no longer needed, or when changes occur that might affect the accreditation of the information system.

(14) Participates in CSPM-sponsored cyber security training within three (3) months of their appointment.

(15) Ensures development, documentation, and presentation of cyber security training for escorts in information systems operational areas.

(16) Ensures that a DAA-approved overwrite method is used for clearing and sanitization, and that a review has been completed of the results of overwrites to verify that the method used completely overwrote all classified or sensitive information.

(17) Ensures that each information system user acknowledges, in writing or electronically, their responsibility (Code of Conduct) for the security of information systems and information.

(18) Communicates individual incident reports to the ISOM to allow the DAA to meet their reporting schedule.

(19) Ensures examination and documentation of suspected cyber security incidents, categorization of incidents as Type 1, Type 2, or No Incident, and retention of documentation.

(20) Ensures analyses of and corrective actions for incidents and findings with status reporting to the DAA.

(21) Conducts self-assessments in accordance with the NNSA PCSP.

(22) Ensures that each individual responsible for major applications within the NNSA Element is aware of and fulfills their cyber security duties, as described in the PCSP and the Element's CSPP.

(23) Recommends changes in the NNSA Element INFOCON status to the DAA.

l. Information System Owner. The information system owner (ISO) is the person or Element responsible for acquiring, operating, or upgrading an information system. The ISO coordinates all aspects of the system for which they are responsible, from initial concept, through development, to implementation and system maintenance. The ISO is also responsible for identifying all information on the

system and is involved with FIPS – level determinations. The information system owner:

(1) Ensures the preparation of the ISSP and the system C&A package.

(2) Ensures the C&A of all information systems under their cognizance.

(3) Ensures implementation of protection measures documented in the ISSP for each information system for which they are the ISSO.

(4) Ensures that privileged users are granted access to information system resources based on the least privilege principle.

(5) Identifies, in coordination with the ISSM, and documents in the ISSP, unique threats to information systems for which they are responsible.

(6) Ensures that the CoL of confidentiality, integrity, and availability for the information is determined prior to use of an information system during the C&A process.

(7) Notifies the ISSM of any changes to the CoL of confidentiality, integrity, and availability for the system.

(8) Documents any special protection requirements identified by the application owner, data owner, or data steward and ensures that these requirements are included within the protection measures implemented in the information system.

(9) For each information system for which they serve as the ISSO, ensures the information system is covered by an ISSP.

(10) Maintains a copy of the ISSP for each information system for which they are the ISSO.

(11) Ensures that all information system security-related documentation is current and accessible to properly authorized individuals.

(12) Ensures the implementation of procedures as defined in the Element CSPP and the ISSP for each information system for which they are the ISSO.

(13) Ensures that system recovery processes are monitored to ensure that security features and procedures are properly restored.

(14) Ensures that the cognizant ISSM is notified when an information system is no longer needed or when changes occur that might affect the accreditation of the information system.

(15) Ensures that information access controls and cyber protection measures are implemented for each information system as described by its ISSP.

(16) Ensures that users and Systems Administrators are properly trained in information system security by identifying cyber security training needs and the personnel who need to attend the cyber security training program.

(17) Conducts cyber security reviews and tests to ensure that cyber security features and controls are functioning and effective.

(18) Participates in the ISSM's self-assessment and training programs.

(19) Ensures that risk assessment is completed for information systems for which they are responsible.

(20) Communicates individual incident reports to the ISSM to allow the ISSM to meet their reporting schedule.

(21) Ensures the implementation of all applicable protection measures for each information system for which they are responsible.

(22) Ensures that unauthorized personnel are not granted use of, or access to, the information system.

(23) Report immediately all security incidents and potential vulnerabilities involving the information to the appropriate ISSM.

m. Information System Security Officer (ISSO). The following roles and responsibilities apply to all information systems for which the ISSO is responsible. The ISSP may be a privileged user. Multiple information systems may be assigned to a single ISSO.

(1) Ensures implementation of protection measures documented in the ISSP for each information system for which they are the ISSO.

(2) Ensures that privileged users are granted access to information system resources based on the least privilege principle.

(3) Identifies, in coordination with the ISSM, and documents in the ISSP, unique threats to information systems for which they are responsible.

(4) Ensures that the CoL of confidentiality, integrity, and availability for the information is determined prior to use of an information system during the C&A process.

(5) Notifies the ISSM of any changes to the CoL of confidentiality, integrity, and availability for the system.

(6) Documents any special protection requirements identified by the application owner, data owner, or data steward and ensures that these requirements are included within the protection measures implemented in the information system.

(7) Ensures each information system for which they are the ISSO is covered by an ISSP.

(8) Maintains a copy of the ISSP for each information system for which they are the ISSO.

(9) Ensures that all information system security-related documentation is current and accessible to properly authorized individuals.

(10) Ensures the implementation of procedures as defined in the Element CSPP and the ISSP for each information system for which they are the ISSO.

(11) Ensures that system recovery processes are monitored to ensure that security features and procedures are properly restored.

(12) Ensures that the cognizant ISSM is notified when an information system is no longer needed, or when the changes occur that might affect the accreditation of the information system.

(13) Ensures that information access controls and cyber protection measures are implemented for each information system as described by its ISSP.

(14) Ensures that users and Systems Administrators are properly trained in information system security by identifying cyber security training needs and the personnel who need to attend the cyber security training program.

(15) Conducts cyber security reviews and tests to ensure that cyber security features and controls are functioning and effective.

(16) Participates in the ISSM's self-assessment and training programs.

(17) Ensures that risk assessment is completed for information systems for which they are responsible.

(18) Communicates individual incident reports to the ISSM to allow the ISSM to meet their reporting schedule.

(19) Ensures the implementation of all applicable protection measures for each information system for which they are responsible.

(20) Ensures that unauthorized personnel are not granted use of, or access to, the information system.

(21) Report immediately all security incidents and potential vulnerabilities involving the information to the appropriate ISSM.

n. Enterprise System and Major Application Manager. The following items apply only to the Enterprise System and Major Application:

(1) Ensures adequate resources are allocated for cyber security of the system or application.

(2) Monitors the effectiveness of cyber security through self-assessments and reviews.

(3) Ensures the development and maintenance of the Enterprise ISSP and the system certification and accreditation package.

(4) Coordinates the ISSP with the involved NNSA Element managers.

(5) Coordinates the ISSP with the Element's ISSM.

(6) Ensures the NNSA Elements' ISSM, ISSO, users, and System Administrators involved with the Enterprise System and Major Application are trained in their specific duties and responsibilities with respect to the Enterprise System and Major Application.

(7) Ensures that the record copy of the Enterprise System and Major Application ISSP is maintained.

(8) Ensures the distribution, as needed, of the Enterprise System and Major Application ISSP to other NNSA Elements.

o. Application Owners and Data Stewards. These roles and responsibilities apply to all information systems.

(1) Determine and declares the sensitivity of the information prior to the information being created, processed, stored, transferred, or accessed on the information system.

(2) Identify unique threats to their information and ensure that this information is forwarded to the ISSO and ISSM.

(3) Advise the ISSO of any special confidentiality, integrity, or availability protection requirements for the information.

(4) Ensure that the information is processed only on a system that is approved at a level appropriate to protect the information.

(5) Determine and document the data and application(s) essential to fulfill the organizational mission, and ensure that requirements for contingencies are determined, implemented, and tested.

(6) Approve access to their information.

(7) Ensure applications and/or data supporting Critical Infrastructure or Key Resources are identified.

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

(9) Provide resources to support Business Continuity for the application data.

p. Users. The roles and responsibilities apply to all cyber assets.

(1) Comply with the requirements of the NNSA PCSP, the NNSA Element's CSPP, and the information system ISSP.

(2) Be aware of, and knowledgeable about, their responsibilities in regard to information systems security.

(3) Ensure that any authentication mechanisms, including passwords, issued for the control of their access to information and information systems, are not shared and are protected at the same level of protection applied to the information to which it permits access, and report any compromise or suspected compromise of an authenticator to the appropriate ISSO. Note that this approach would not apply for RSA tokens.

(4) Be responsible and accountable for their actions on an information system.

(5) Acknowledge, via electronic signature or in writing, their responsibilities (Code of Conduct) for protecting information systems and classified information.

(6) Participate in training on the information system's prescribed security restrictions and safeguards before initial access to a system. Additionally, participate in an ongoing security education, training, and awareness program.

(7) Immediately report all security incidents and potential threats and vulnerabilities involving the information system to the appropriate personnel.

(8) Ensure that system media and system output are properly classified, marked, controlled, and stored.

(9) Protect terminals from unauthorized access, as described in the information system ISSP.

(10) Inform the ISSO when access to a particular information system is no longer required, for example, completion of a project, transfer, retirement, or resignation.

(11) Observe rules and regulations governing the secure operation and authorized use of information systems.

(12) Use the information system only for official government business or other activities authorized by NNSA or the NNSA Element manager.

(13) Receive electronic or written permission from the DAA before any attempt to bypass or test security mechanisms.

q. Privileged Users and System Administrators.

(1) All privileged users must be responsible for all requirements stated for general users.

(2) Privileged users are responsible to ensure that user access to the information system's resources and information is based on the least privilege principle.

(3) All privileged users must:

(a) Be U.S. citizens, unless otherwise approved in accordance with the approved NNSA Element ISPP or in writing by the cognizant DAA. Foreign Nationals are explicitly prohibited from being privileged users on classified systems

(b) Possess approvals of Need-to-Know for all information on the system.

(c) Possess an Access Authorization sufficient for access to the highest classification and most restrictive category of data processed on the information system.

(d) Use unique identifiers as described in the information system ISSP.

(e) Protect the root or super-user authenticator at the highest level of data it secures.

(f) Be responsible for all super-user or root actions under their account.

(g) Report any and all security relevant information system problems to the ISSO.

(h) Use the special access or privileges granted only to perform authorized tasks and functions.

r. Certification Agent (CA)/Certifier. The Certification Agent, or Certifier, is designated to perform security certification. The ISSM may fulfill the role of the CA. General duties of the Certifier include:

(1) Ensures that risk assessments and security evaluations are completed prior to information system, network, and application certification.

(2) Certifies the extent to which systems, networks and applications meet prescribed security requirements.

(3) Prepares the certification report and, upon the completion of certification, forwards the report to the DAA through the CA, if the ISSM is not the CA, with their recommendation on accreditation.

(4) Ensures Corrective Action Plans (CAPs) are prepared.

(5) Maintains and provides other records and reports of certification activities, as necessary.

(6) Reviews all information contained in the ISSP.

(7) Conducts a comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards made in support of the accreditation process to establish the extent to which a particular design and implementation meets a set of specified security requirements.

(8) Submits recommendations on C&A package to the DAA.

This page left intentionally blank.

CHAPTER III. CONFIGURATION MANAGEMENT

1. INTRODUCTION. Configuration Management (CM) applies administration, technical direction, and surveillance to identify and document functional and physical characteristics of a configuration item, to control changes, record and report change processing and implementation, and to verify compliance with specified requirements. Configuration management implements measures to ensure that protection features specified in NNSA-approved minimum information system security configurations are implemented in the system and maintained in the instantiation of system components by applying a level of discipline and control to the process of system maintenance and modification. The minimum set of security controls for unclassified and classified information systems, as determined by the system categorization, is detailed in NAP 14.2-C, Chapter III, NNSA Certification and Accreditation (C&A) Process.

2. REQUIREMENTS. The NNSA Element must implement the following NNSA CM processes for all information systems within the Element.

   a. Design documentation and any acquisition specifications that must identify the minimum security configuration for the information system, or applicable components of the information system requiring security configurations when being purchased.

      If it is necessary to develop alternative minimum security configurations due to operational or mission requirements, the new configuration must be selected from recognized sources of checklist-producing organizations, including NIST[1], the National Security Agency (NSA)[2], the DISA Security Technical Implementation Guides (STIGs), and the Center for Internet Security (CIS) benchmarks[3]. Such alternative configurations must be approved by the cognizant DAA.

   b. The Element's CM procedures for maintaining documentation, tracking changes, approving configuration changes, and implementing vulnerability and patch management shall be described in the Element CSPP.

   c. The minimum set of security controls identified for an information system must be described in CM documentation which includes ISSPs, Contingency Plans, ST&E Procedures, user and administrative guidance, and system component inventories.

1

1 The NIST checklist repository is located at http://checklists.nist.gov/ .
2 The NSA's checklists are available at http://www.nsa.gov/ia/.
3 CIS's site is http://www.cisecurity.org/.

d. The Element's CM procedures, monitoring capability to continuously detect and manage software changes, roles and responsibilities, and configuration identifiers shall be documented in a Configuration Management Plan(s) (CMP). The CMP shall describe the methodology and procedures used for configuration controls to include at a minimum, the following:

(1) Identification of the roles and responsibilities for change approval or disapproval.

(2) Information system and configuration item unique identification and labeling.

(3) Configuration change identification, tracking, control, and history.

(4) Configuration auditing and status accounting.

(5) Vulnerability and patch management.

(6) Security configuration checklist for operating system software, application software, and hardware platforms.

(7) Documentation of the methodology and tools used to monitor configuration changes.

e. Documentation of Minimum Security Configurations requires implementation of the minimum set of security controls is addressed, as required by the system's security categorization. These controls are listed in NAP 14.2-C, *NNSA Certification and Accreditation (C&A) Process*.

f. Organizations using Microsoft Windows XP and plan to upgrade to Vista must adopt the security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DOD) and the Department of Homeland Security (DHS).

g. If it is necessary to develop alternative minimum security configurations due operational or mission requirements, the new configuration must be selected from recognized sources of checklist-producing organizations, including NIST[4], the National Security Agency (NSA)[5], the DISA Security Technical Implementation Guides (STIGs), and the Center for Internet Security (CIS) benchmarks[6]. Such alternative configurations must be approved by the cognizant DAA.

2

4 The NIST checklist repository is located at http://checklists.nist.gov/ .
5 The NSA's checklists are available at http://www.nsa.gov/ia/.
6 CIS's site is http://www.cisecurity.org/.

CHAPTER IV. CYBER SECURITY PROGRAM PLAN

1. INTRODUCTION. The NNSA CSPP is the document that outlines the policies, procedures, and practices of an organization's (e.g., an NNSA site) CSP—classified and unclassified. The CSPP is a top-level, stand-alone program document at the management level and details the organization's policies, procedures, and practices for ensuring effective cyber security. It also explains the organization's specific environment, missions, and threats. The CSPP will be integrated with other program plans in the Element, such as Site Safeguards and Security Plan (SSSP), and the Information Resource Management (IRM) plans.

2. CSPP CONTENTS. The CSPP must describe how the organization implements the NNSA PCSP. The CSPP must explain the organization's specific environment, missions, and threats and describe the policies, procedures, and practices for ensuring effective cyber security. If the following requirements can be met with existing organization policies or procedures, they should be summarized and referenced in the CSPP and a copy attached to the CSPP.

   a. Environment. Describe the site's mission, objectives, and security environment.

   b. Information Types and Groups. Identify the Information Types and/or Groups. See Chapter V for a description of the Information Types and/or Groups handled by the site.

   c. Site Unique Threats. Reference or document any threat or threat assessments used as the basis for its threat environment, such as the NNSA Threat Assessment, OPSEC Threat Assessments, and Site Unique Threats.

   d. Roles and Responsibilities. Define the cyber security roles and responsibilities for the site, such as the ISSM, ISSO, system administrator, Certification Agent, and general user. Cyber security training requirements for all participants are provided in CNSSD-500 Information Assurance (IA) Education, Training, and Awareness - dated August 2006; and NSTISSD-501 National Training Program for Information Systems Security (INFOSEC) Professionals - dated 16 November 1992.

   e. Program and Project Controls and Accountability. Describe the method for tracking the site's implementation of the NNSA PCSP in terms of cost and schedule.

   f. Plan of Actions and Milestones (POA&M). Describe the site's process for tracking system-level weaknesses to include corrective action plans to track the completion of milestones.

g. Information Systems. Reference an inventory of information systems: accredited, in the accreditation process, and not accredited.

h. C&A Program. Describe the site's information system C&A process to include processes for additional instantiations of accredited systems. Include (ISSP) format requirements.

i. Equipment and Software Management.

(1) Configuration Management.

(a) Describe the site's CM policies and procedures.

(b) Identify any NNSA-approved minimum information system security configurations implemented in the Element's information systems.

(c) Describe the site's process for identifying and managing information system configurations that cannot apply NNSA-approved minimum information system security configurations due to operational or mission requirements.

(d) Describe the site's process for planning, documenting, and managing system interconnections to include:

i. Purpose and baseline configuration of the interconnection.

ii. Methods used to meet the security requirements of interconnected systems and/or adjudicate security implementation differences between the systems.

iii. Processes for mutual configuration management, change notification, maintenance, incident response, and operation of the interconnection.

iv. Process for governing the creation, maintenance, and approval of Interconnection Agreements.

(2) Equipment Maintenance. Describe the maintenance policies and procedures, including the introduction of vendor maintenance hardware, software and firmware, and the management of remote maintenance activities.

(3) Sanitization – Clearing, Purging, and Destruction. Describe the Element's management, operational, technical, and assurance controls for sanitization.

Provide the DAA-approved process for the following:

(a) Clearing, purging, and destroying information system storage media, memory devices, and other related hardware components.

(b) Reuse of information storage media, memory devices, and other related hardware components at a lower classification or sensitivity level.

j. Decommissioning. Describe the procedures for decommissioning information systems.

k. Incident Handling. Describe the composition of the site incident response team, contact methods, such as telephone numbers, pagers, cell phones, e-mail, and incident handling and reporting procedures.

l. Information Condition. Describe the process for establishing, changing, and reporting the site's INFOCON status. Describe the site's response measures for each INFOCON level. Describe the incident warning and advisory response process for the site.

m. Security Monitoring. Describe the site's security monitoring policies, processes, and procedures, including how monitoring is used to mitigate risks to the site. Describe the site's processes and procedures for detecting and managing intrusion detection at the desktop, network, and site levels.

n. Security Coordination. Describe the site's process and procedures to ensure coordination with other security programs, such as physical security; personnel security; Technical Surveillance Countermeasures (TSCM); TEMPEST; Classified Matter Protection and Control (CMPC); Protected Transmission System (PTS); Operations Security (OPSEC); and Computer Security (COMSEC).

o. Malicious Code. Describe the site's process and procedures to address malicious code incidents (e.g., incidents handled at the boundary, at desktops, and at selected locations), the mechanisms employed, and frequency of updating anti-malicious code software throughout the site.

p. Denial of Service and/or Continuity of Service. Describe the business impact analysis (BIA) process for identifying those information systems and networks that have a low tolerance for disruption or unavailability (system criticality), and the procedures and mechanisms that will be employed to limit and recover from such disruption or unavailability.

q. Internet Security. Describe the site's Internet use policy, method of securing the site's network from external threats via the Internet connection, policies and procedures for reviews of Web page and server content, as well as Web page and server monitoring policy.

r. E-mail. Describe the site's e-mail policy, including controls for the use of offsite e-mail.

s. Component and Output Marking and Labeling. Describe the site's policy for marking and labeling the sensitivity or classification levels of computers, computer equipment, media storage devices, and computer output.

t. Clear Text Password Management. Describe the site's program for the elimination of clear text passwords from existing and future information systems.

u. Data Backup and Restoration. Describe the site's policies for data backup and restoration.

v. Disaster Recovery Program. Describe the site's disaster recovery program, including integration of information systems, Continuity of Service plans, and the procedures for regular testing of continuity of operations and contingency plans.

w. Output and Display Device Access. Describe the site's policies for controlling access to system output and display devices.

x. Portable Hardware and Software Technical Reviews. Describe the process for performing technical reviews of the hardware and software components of portable computers that are taken or used outside the U.S. or may have been under the control of a non-U.S. Government organization.

y. Portable Computing Devices. Describe the policies and procedures for managing the use of portable computing devices in all areas of the site.

z. External Information Systems. Describe the policies and procedures for managing the use of external information systems in all areas of the site.

aa. Wireless Information Systems. Describe the policies and procedures for managing installation and use of Radio Frequency (RF) and Infrared (IR) systems in all areas of the site.

ab. Risk Management. Describe the site's process for risk management for all information systems and information system components.

ac. Remote Access. Describe management, operational, technical, and assurance controls for remote access.

ad. Training. Describe the process for cyber security training and awareness programs, including who must receive training and how frequently re-training will occur. Describe the methodology being used for training, such as briefings or e-mail. Identify those positions requiring training, and identify by title or position those responsible for overseeing training activities at the site.

ae. Performance Assessment. Describe the site's process and metrics employed to assess compliance with the CSPP and the process for evolving these metrics. Describe the site's peer review and self-assessment processes, including frequency of reviews, the process for selecting peer review members, qualifications required of the prospective individuals or entities, and who is responsible for selecting peer review participants.

af. Plan Change Management. Describe the update frequency for the CSPP and the process for updating the plan.

ag. Downloading Unclassified Files from an Unclassified System. Describe the procedure for downloading unclassified data from classified system.

This page intentionally left blank.

CHAPTER V. INFORMATION GROUPS

1. INTRODUCTION. Unclassified Information and National Security Information Groups contain all information that requires similar protection or is similar in content or use. The following have been defined for use in assessing the cyber threats to information, and for use in defining the minimum protection criteria.

   a. Unclassified Information Types.

      (1) Open, Public, and Unrestricted Access. Information that requires no protection from disclosure, such as information approved for public release.

      (2) Unclassified Protected. Unclassified information that has been determined by the data owner or data steward to require additional protection due to its sensitive subject matter or impact to Departmental or organizational missions.

      (3) Unclassified Mandatory Protection and SUI. Information requiring additional protections as mandated by policy or laws, such as the following:

         (a) Privacy Act information.

         (b) Agreements between DOE, NNSA, its contractors, and other entities, such as commercial organizations or foreign governments, i.e., Cooperative Research and Development Agreement (CRADA).

         (c) Proprietary information (but not third party proprietary).

         (d) Unclassified Controlled Nuclear Information (UCNI).

         (e) Export-controlled information (ECI).

         (f) Naval Nuclear Propulsion Information (NNPI).

         (g) Military and dual use information, such as the Critical Military Technology and Materials list identified by the Department of Defense (DOD).

         (h) Nonproliferation information.

         (i) Official Use Only.

         (j) Personally Identifiable Information (PII) – Refer to Chapter XVII for a complete definition of PII.

b. National Security Systems Information Groups.

(1) Confidential or Secret Non-Nuclear Weapons. Information classified Confidential National Security Information, Confidential Restricted Data, Confidential Formerly Restricted Data, Secret National Security Information, or Secret Formerly Restricted Data and does not contain any nuclear weapons data but may contain information related to uranium enrichment.

(2) Secret Restricted Non-Nuclear Weapons Data. Information classified Secret Restricted Data and does not contain any nuclear weapons data, but it may contain information related to uranium enrichment or other Secret Restricted Data.

(3) Confidential Restricted Data Sigmas 1 through 13, and 15, and 20. Information classified as Confidential and identified as Restricted Data, Formerly Restricted Data, or is related to nuclear weapons. This information is further marked with at least one of the sigma categories 1 through 13.

(a) Sigmas 1 and 2**.** Theory of operation or complete design of hydrodynamic, nuclear, fission weapons or their unique components. This includes the high explosive system with its detonators and firing unit, pit system, and nuclear initiation system as they pertain to weapon design and theory.

(b) Sigmas 3, 4, 5, 9, 10, 11, 12, and 13, 15 and 20**.** Manufacturing and utilization information not comprehensively revealing the theory of operation or design of the physics package; information inherent in pre-shot and post-shot activities necessary in the testing of atomic weapons or devices; production rate and/or stockpile quantities of nuclear weapons and their components; general studies not directly related to the design or performance of specific weapons or weapons systems such as reliability studies, fusing studies, damage studies, aerodynamic studies; chemistry metallurgy, and processing of materials peculiar to the field of atomic weapons or nuclear explosive devices; Information concerning inertial confinement fusion that reveals or is indicative of weapon data; Theory of operation or complete design of the nuclear energy converter, energy director, or other nuclear directed energy weapon outside the radiation case of the nuclear source but within the envelope of the nuclear directed energy weapon concept; and manufacturing and utilization information for nuclear energy converters, directors, or other nuclear directed energy weapon outside the nuclear source radiation case, not comprehensively revealing the theory of operation or design of the nuclear directed energy weapon concept.

(4) Secret Restricted Data Sigmas 1 through 13.. Information classified as Secret and identified as Restricted Data and related to nuclear weapons. This information is further marked with at least one of the Sigma categories 1 through 13, 15, and 20.

(a) Sigmas 1 and 2. Theory of operation or complete design of hydrodynamic, nuclear, fission weapons or their unique components. This includes the high explosive system with its detonators and firing unit, pit system, and nuclear initiation system as they pertain to weapon design and theory.

(b) Sigmas 3, 4, 5, 9, 10, 11, 12, and 13. Manufacturing and utilization information not comprehensively revealing the theory of operation or design of the physics package; information inherent in pre-shot and post-shot activities necessary in the testing of atomic weapons or devices; production rate and/or stockpile quantities of nuclear weapons and their components; general studies not directly related to the design or performance of specific weapons or weapons systems – reliability studies, fusing studies, damage studies, and aerodynamic studies; chemistry and metallurgy, and processing of materials peculiar to the field of atomic weapons or nuclear explosive devices; information concerning inertial confinement fusion that reveals or is indicative of weapon data; theory of operation or complete design of the nuclear energy converter, energy director, or other nuclear directed energy weapon outside the radiation case of the nuclear source but within the envelope of the nuclear directed energy weapon concept; and manufacturing and utilization information for nuclear energy converters, directors, or other nuclear directed energy weapon outside the nuclear source radiation case, not comprehensively revealing the theory of operation or design of the nuclear directed energy weapon concept.

(c) Sigma 15. The category of sensitive information concerning design and function of nuclear weapons use control systems, features, and their components. This includes use control information for passive and active systems.

(d) Sigma 20. The category of nuclear weapon data that pertains to sensitive improvised nuclear device information.

(5) Secret Restricted Data Sigma 14. Information that is classified as Secret and identified as Restricted Data or is related to nuclear weapons. Sigma 14 is the category of sensitive information concerning the vulnerability of nuclear weapons to deliberate unauthorized nuclear detonation.

(6) Top Secret. Information classified Top Secret NSI, Top Secret FRD, or Top Secret Restricted Data that does not pertain to Nuclear Weapons.

(7) Top Secret Restricted Data. Nuclear Weapon information classified Top Secret.

(8) Special Information Groups. These Information Groups contain Confidential or Secret Restricted Data (or other National Security data) that the US Government, DOE, or NNSA have determined that special or additional protection is necessary.

CHAPTER VI. NNSA CYBER SECURITY PROGRAM DEVIATIONS

1. INTRODUCTION. This chapter describes the types of deviations, such as variances, waivers, and exceptions, required justifications, and the process for obtaining deviations from the NNSA PCSP requirements.

2. CRITERIA AND PROCESSES. All approved deviations, as described below, must be documented in the ISSP for the information system, the SSSP, or the Site Security Plan, as appropriate.

   a. Variances. Variances are approved conditions that technically vary from a NNSA PCSP requirement but afford equivalent levels of protection.

      (1) Variance requests must be submitted in writing to the DAA. The variance request must include a detailed description of the requirement(s) and rationale. The variance documentation must be referenced in the ISSP.

      (2) The cognizant DAA will review and approve in writing, or the cognizant DAA will disapprove with comments and recommendations.

      (3) Variances may be approved for up to three (3) years and documented in the ISSP, but they must be submitted for reconsideration whenever the information system is accredited or re-accredited.

   b. Waivers. Waivers are approved, non-standard conditions that deviate from a NNSA PCSP requirement, which, if uncompensated, would create a potential or real cyber security vulnerability. Waivers require implementation of compensatory measures that will be in effect for the duration of the waiver.

      (1) Waiver requests and supporting documentation must be submitted in writing to the cognizant DAA for review.

      (2) Documentation supporting the waiver request must identify the requirement(s) to be waived, indicate the compensatory measures implemented, and, if appropriate, indicate that performance testing has been completed to validate the compensatory measures.

      (3) The DAA will forward the waiver request and documented recommendation for approval to the NNSA CSPM.

      (4) The NNSA CSPM will approve or disapprove the waiver request and provide a final decision in writing to the cognizant DAA.

      (5) The cognizant DAA will notify the ISSM.

(6) Approved waivers may remain in effect for up to the expiration of the C&A, which may be less than two years to a maximum of three years. Approved waivers must be referenced in the ISSP. If an extension is necessary, the waiver request must be re-submitted.

c. Exceptions. Exceptions are approved deviations from an NNSA PCSP requirement that creates a security vulnerability. Exceptions shall only be approved when correction of the condition is not feasible or cost effective and compensatory measures are inadequate to preclude the acceptance of risk by the cognizant DAA.

(1) Requests for exceptions and supporting documentation must be submitted in writing to the cognizant DAA for review.

(2) Documentation supporting the exception request must identify the requirement(s) that cannot be met, indicate any compensatory measures implemented, and, if appropriate, indicate that performance testing has been completed to validate the compensatory measures.

(3) The DAA will forward the exception request and documented recommendation for approval to the NNSA CSPM.

(4) Exceptions must be documented in the ISSP.

(5) The NNSA CSPM, or higher authority, will approve or disapprove the exception request and provide a final decision in writing to the cognizant DAA.

(6) The cognizant DAA will notify the ISSM.

(7) Approved exceptions may remain in effect for one year.

(8) The cognizant DAA must review and validate the need for each exception.

CHAPTER VII. INCIDENT MANAGEMENT

1. INTRODUCTION. This chapter establishes the minimum criteria and processes for reporting and responding to cyber security incidents involving NNSA information systems.

2. REPORTING CRITERIA AND PROCESSES.

   a. Reportable Cyber Security Incidents. The site's CSPP must document the processes for reporting cyber security incidents that are IMI-1 and IMI-2. Cyber security-related incidents must be coordinated with Safeguards and Security. In addition, cyber security-related incidents must be reported that meet one or more of the following criteria:

      (1) Incidents of Security Concern. Report the cyber security aspects of the following Incidents of Security Concern involving National Security Systems, as adapted from DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.

         (a) Impact Measurement Index (IMI-1). Report incidents that pose an immediate danger or short-term threat to National Security interests and/or critical NNSA or DOE assets, that potentially create a serious security situation, or that create high media visibility interest. The following cyber security incidents must be reported according to the procedures in this NAP, in addition to the reporting requirements in DOE M 470.4-1. These incidents must be reported within one working hour of discovery.

            (i) Confirmed or suspected loss, theft, diversion, or unauthorized release of Weapon Data contained in an information system or on cyber media.

            (ii) Confirmed or suspected loss, theft, diversion, unauthorized release of TOP SECRET information or Special Access Program (SAP) information contained in an information system or on cyber media.

            (iii) Confirmed or suspected intrusions, hacking, or break-ins into NNSA information systems containing TOP SECRET or SAP information.

         (b) Impact Measurement Index (IMI-2). Report incidents that pose a near- or long-term threat to National Security interests and/or critical NNSA or DOE assets, or incidents that potentially create a crisis or dangerous situation. The following cyber security incidents must be reported according to the procedures in this

NAP, in addition to any other reporting. These incidents must be reported within eight working hours of discovery.

(i) Confirmed or suspected intrusions, hacks, or break-ins into NNSA information systems or cyber media, containing Confidential Non-Nuclear Weapons Information or Secret Restricted Data Information.

(ii) Confirmed or suspected intrusions, hacking, or break-ins into NNSA information systems or cyber media containing Confidential Non-Nuclear Weapons Information or Secret Restricted Data Information.

(iii) Loss of classified information that must be reported to other Government agencies or foreign associates.

(iv) The loss of any DOE classified information involving NNSA information systems or cyber media, which requires State or local government or other Federal agency notification.

(c) Impact Measurement Index (IMI-3). Report incidents that pose long-term threats to NNSA or DOE security interests, or incidents that could potentially degrade the overall effectiveness of the NNSA or the Department's protection programs. The following cyber security incidents must be reported according to the procedures in this NAP, in addition to any other reporting. These incidents must be reported within eight working hours of discovery.

(i) Confirmed or suspected unauthorized disclosure, loss or potential loss of CONFIDENTIAL matter via intrusions, hacking, or break-ins into NNSA information systems or cyber media.

(ii) Confirmed or suspected unauthorized disclosure, loss/potential loss of Unclassified Mandatory Protection Information via intrusions, hacking, or break-ins into NNSA information systems or loss/potential loss of cyber media.

Table VII-1 on the following page provides the incident reporting requirements for Incidents of Security based on the IMI.

Table VII-1. Required Time Frame for Reporting Incidents of Security Concern Based on Impact Measurement Index

IMI Designation	Time Frame
IMI-1	Within 1 working hour of discovery
IMI-2	Within 8 working hours of discovery
IMI-3	Within 8 working hours of discovery

(2) Incidents of NNSA Cyber Security Concern. These incidents must be reported based on the Type and System Impact Category, as defined below. Incidents may be, but are not limited to, the result of cyber security alerts received and investigated by the site.

(a) Type 1 incidents are successful incidents that potentially create serious breaches of DOE and/or NNSA cyber security, or have the potential to generate negative media interest. The following are the currently defined Type 1 incidents.

(i) Compromise or Intrusion. All unintentional or intentional instances of system compromise or intrusion by unauthorized persons must be reported, including user-level compromises, root (administrator) compromises, and instances in which users exceed privilege levels.

(ii) Web Site Defacement. All instances of a defaced Web site must be reported.

(iii) Malicious Code. All instances of successful large network site-wide infection, or persistent attempts at infection by malicious code, such as viruses, Trojan horses, or worms, must be reported.

(iv) Denial of Service. Intentional or unintentional denial of service (successful or persistent attempts) that affects or threatens to affect a critical service, or that denies access to all or one or more large portions of a network, must be reported.

(v) Critical Infrastructure Protection (CIP). Any activity that adversely affects an asset identified as critical infrastructure must be reported. NNSA CIP assets are determined by the NNSA Administrator.

(vi) Unauthorized Use. Unauthorized use should be construed as any activity that adversely affects an information system's normal, baseline performance and/or is not recognized as being related to NNSA's mission. For

example, unauthorized use can be using a DOE or NNSA computer to obtain Government data without authorization. Unauthorized use can involve using systems to break the law. Unauthorized use includes, but is not limited to, port scanning that excessively degrades performance. Note that these activities may only be performed when authorized by the DAA: IP (Internet protocol) spoofing; network reconnaissance; monitoring; hacking into servers; running traffic-generating applications that generate unnecessary network broadcast storms or drive large amounts of traffic to computers; or using illegal (or misusing copyrighted) software images, applications, data, and music.

(b) Type 2 incidents are attempted incidents that pose potential long-term threats to DOE and/or NNSA cyber security interests, or that may degrade the overall effectiveness of the Department's cyber security posture. The following are the currently defined Type 2 incidents.

(i) Attempted Intrusion. A significant and/or persistent attempted intrusion that stands out above the daily activity or noise level, as determined by the system owner, and that would result in unauthorized access (compromise) if the system were not protected.

(ii) Reconnaissance Activity. Persistent surveillance and resource mapping probes and scans that stand out above the daily activity or noise level and represent activity that is designed to collect information about vulnerabilities in a network and map network resources and available services.

b. System Impact Categories. System impact categories characterize the potential impact of incidents that compromise DOE or NNSA information and information systems. Such incidents may impact DOE or NNSA operations, assets, individuals, missions, or reputations. System impact categories identify the level of sensitivity and criticality of information and information systems by assessing the impact of the LOC, integrity, and availability. Performing this impact analysis is a fundamental step in risk assessment. Each of the security objectives, such as confidentiality, integrity, and availability, is assessed according to categories in Table VII-2 on the following page.

(1) Low Impact. Loss of system confidentiality, integrity, and availability could be expected to have a limited adverse effect on DOE or NNSA operations, assets, or individuals, requiring minor corrective actions or repairs.

(2) Moderate Impact. Loss of system confidentiality, integrity, and availability could be expected to have a serious adverse effect on DOE or NNSA operations, assets, or individuals, including significant degradation or major damage, requiring extensive corrective actions or repairs.

(3) High impact. Loss of system confidentiality, integrity, and availability could be expected to have a severe or catastrophic adverse effect on DOE and NNSA operations, assets, or individuals. The incident could cause the loss of mission capability for a period that poses a threat to human life or results in the loss of major assets.

Table V11-2. Required Time Frame for Reporting Cyber Security Incidents to the Information Assurance Response Center (IARC)

	System Impact Category		
Incident Type	**Low**	**Moderate**	**High**
Type 1	Within 4 hours	Within 1 hour	Within 1 hour
Type 2	Within 1 week	Within 24 hours	Within 24 hours
Personally Identifiable Information (PII)*	Within 35 minutes	Within 35 minutes	Within 35 minutes

* Based on mandated reporting requirements for PII, all suspected or confirmed incidents involving PII must be reported within 35 minutes regardless of the Type or System Impact. See definition and examples in Appendix XVIII for further clarification.

Figure VII-1 illustrates the process for reporting NNSA cyber security incidents. For PII, see Figures VII-2 and VII-3.

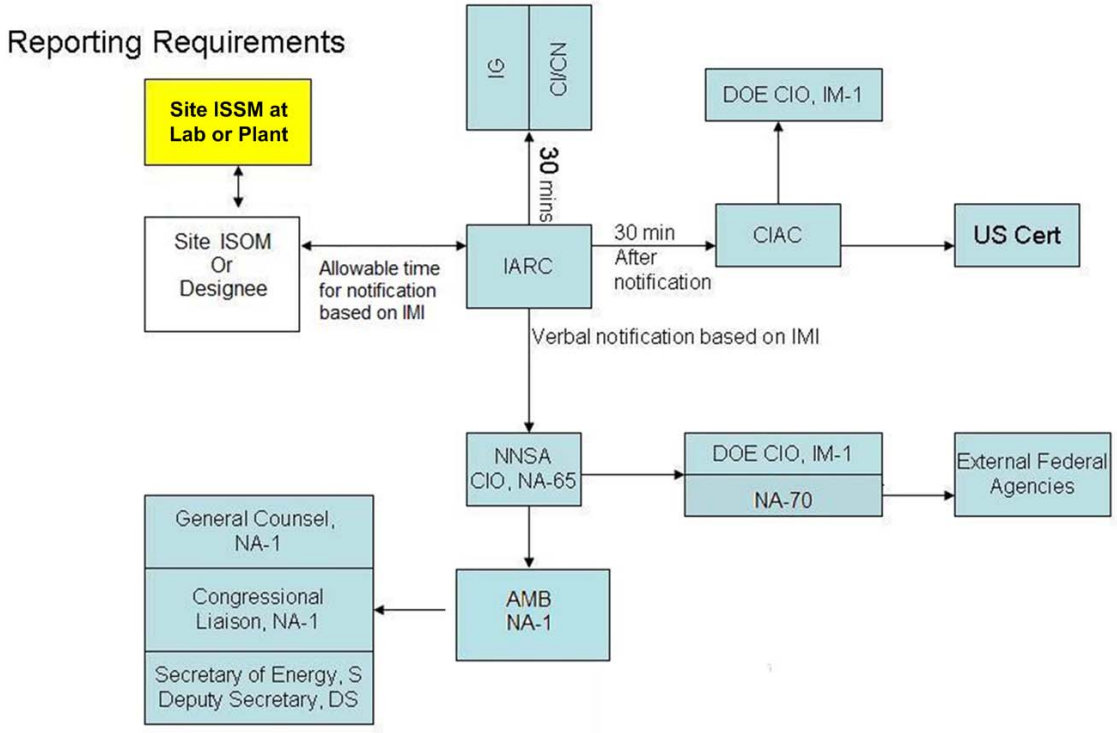


Figure VII-1. NNSA Cyber Security Incident Reporting Process

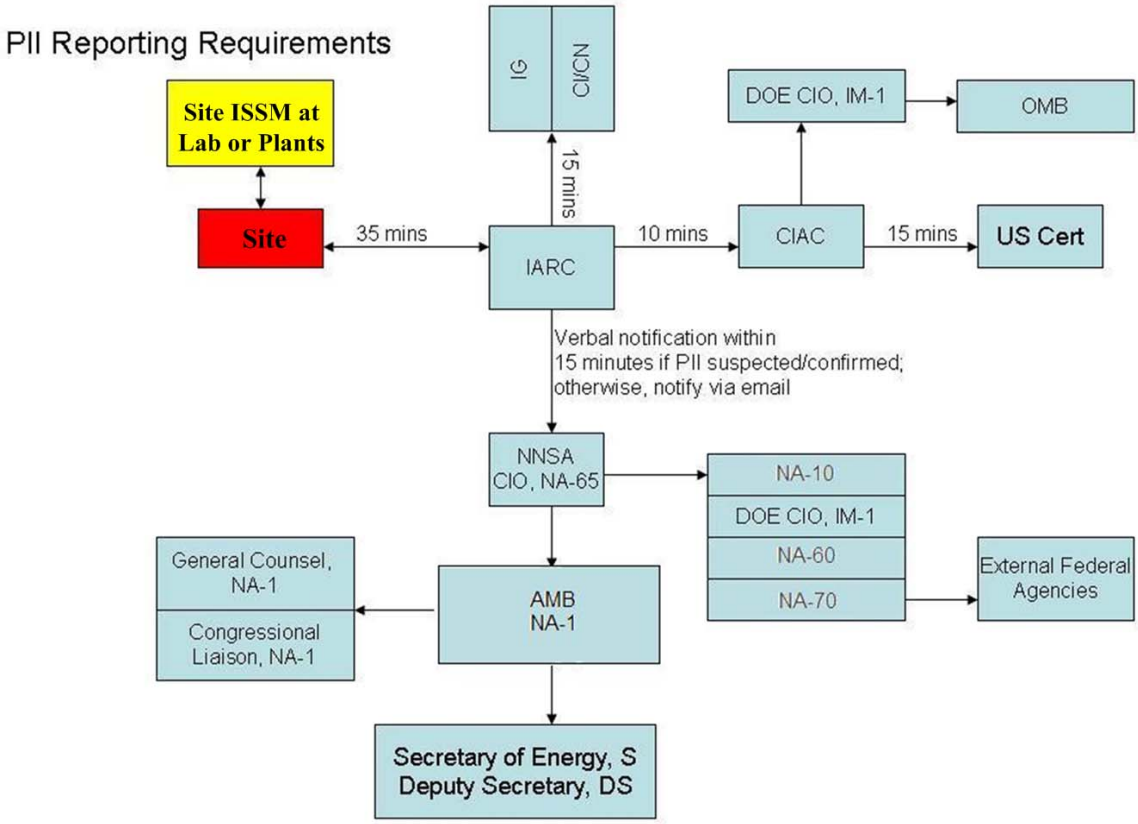


Figure VII-2. NNSA PII Cyber Security Incident Reporting Process

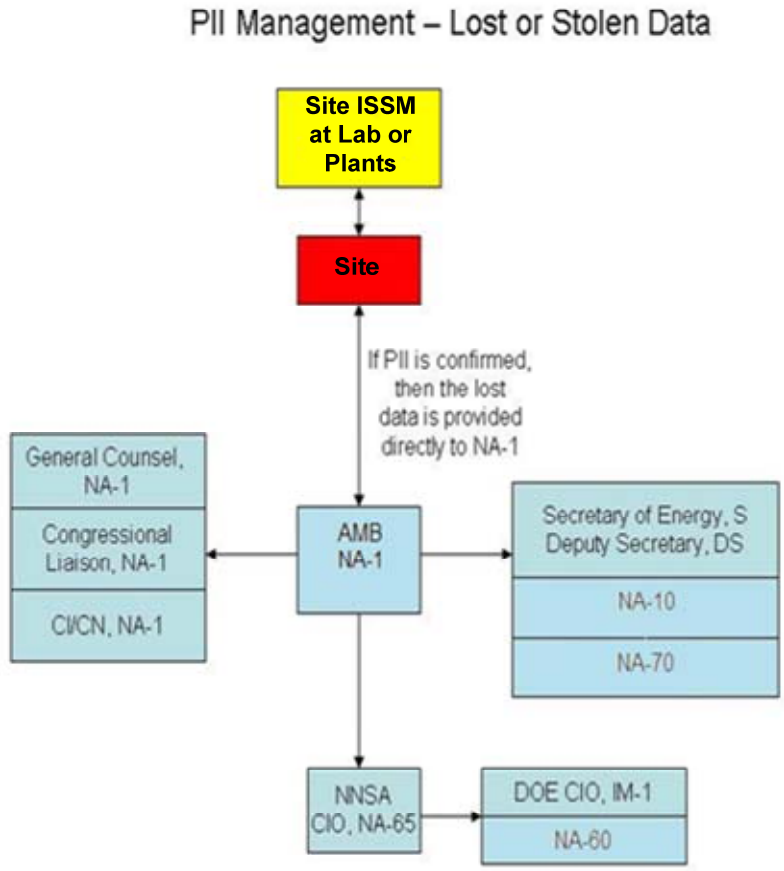


Figure VII-3. NNSA PII Management – Lost or Stolen Data Process Flow

c. The cognizant ISOM must be notified within 24 hours of discovery of an incident by the NNSA site. Monthly reports on the status of incident resolution, whether or not any reportable, successful, or attempted incidents have occurred during the month, must also be transmitted to the ISOM.

d. Cyber Security Incident Report Content. The content and format of an incident report will be specified by the IARC. At a minimum, incident reports must include date(s), time(s), type, source, corrective actions taken, if any, resources affected, site impact, and site point-of-contact. Sources may vary depending on the type of attack, but may include Internet Protocol (IP) address, e-mail address, or other identifying source characteristics. Additional content may be specified by the DAA and/or IARC, as incident situations change.

e. Incidents Involving PII. All suspected or confirmed cyber security incidents involving PII as defined in Appendix B, *Definitions*, must be reported to the

IARC within 35 minutes of discovery. Discovery is defined as the moment that the CSSM or their staff have determined that a reported incident could involve PII. This notification can be verbal or written via e-mail. As additional information is discovered pertaining to the incident, the impacted site must provide IARC with the updated information within 35 minutes. Note that if a primary impacted site has solicited the assistance of another secondary site during the investigation, the primary site has the responsibility for reporting all information to the IARC.

f. Archiving Cyber Security Incident Information. Sites must store all information related to a reportable incident, as defined in paragraph 2.a of this chapter for at least one year. Storage methods, including custody, must comply with applicable evidentiary requirements for possible future law enforcement use.

g. Counterintelligence Reporting. Events identified in DOE O 475.1, *Counterintelligence Program,* must be reported by the IARC to the Office of Intelligence and Counterintelligence (OICI), in accordance with the reporting procedures in DOE O 475.1.

h. Automated Systems. Automated systems may be used to implement these protocols.

3. CIAC CYBER SECURITY ALERTS. Cyber security alerts issued by CIAC shall be investigated, analyzed, and reported as an incident. Positive feedback from the sites is required in response to an alert, and the incident reporting mechanism provides the necessary information.

This page intentionally left blank.

CHAPTER VIII. INFORMATION CONDITION (INFOCON)

1. INTRODUCTION. This chapter describes the minimum preparations and actions required to react uniformly to warnings of cyber security incidents, heighten or reduce the cyber defensive posture, defend against computer network attacks, and mitigate sustained damage to NNSA information and infrastructure, including computer and telecommunications networks and systems. The INFOCON is a comprehensive defense posture and response based on the status of information systems, NNSA operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system impacts all personnel who use NNSA information systems, protects systems while supporting mission accomplishment, and coordinates the overall defensive effort through adherence to standards.

   The INFOCON system presents a structured, coordinated approach to react to adversarial attacks on NNSA information, computer systems, and networks and systems. While all systems are vulnerable to some degree, factors such as low-cost, readily available information technology, increased system connectivity, and remote access capability make Computer Network Attack (CNA) an attractive option to an adversary. CNA is defined as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." INFOCON also outlines countermeasures to scanning, probing, and other suspicious activity, unauthorized access, and data browsing. NNSA INFOCON measures focus on computer network-based protective measures due to the unique nature of CNA. Each level reflects a defensive posture based on the risk to NNSA operations through the disruption of information systems and networks.

2. CRITERIA AND PROCESSES.

   a. Each NNSA site's INFOCON response measure must be documented in the site's CSPP.

   b. INFOCON procedures must be well integrated with the site's Security Condition (SECON) procedures, emergency procedures, Continuity of Operations plans, and incident handling processes.

   c. Cyber security incidents must be reported as described in Chapter VII.

   d. DAAs may evaluate their situation and recommend changes in the INFOCON to the NNSA Site Manager for sites under their cognizance; however, the INFOCON must remain at least at high as the current INFOCON directed by NNSA. If the NNSA Site Manager agrees to the recommended change in INFOCON status, the DAA must report the change to the CSPM within 4 hours.

   e. The CSPM will notify DAA when the NNSA INFOCON is changed, through the most rapid means available, and must notify the CSPM if recommended or directed INFOCON response measures conflict with organization or mission priorities within 2 hours of NNSA determination of INFOCON response measures.

   f. The DAA must disseminate INFOCON information within their organization and

to organizations under their cognizance, through the most rapid means available.

3. NNSA INFOCON. Several critical assumptions were made about the nature of CNA and Computer Network Exploit (CNE) in developing the NNSA INFOCON system. Understanding these assumptions is essential to effective implementation of this system.

   a. Shared Risk. In today's network-centric environment, risk assumed by one NNSA site is risk shared by all. Unlike most other security activities, a successful network intrusion in one NNSA location may, in many cases, facilitate access at other locations. This necessitates a common understanding of the situation and responses associated with the declared NNSA INFOCON. These actions must be carried out concurrently at all NNSA locations for an effective defense.

   b. Advance Preparation. Preparation is key, given the speed and reduced signature of CNA and CNE. Protective measures must be planned, prepared, exercised, and often executed well in advance of an attack. Preventive measures are emphasized in INFOCON responses because there may be little time to react effectively during the attack. Prevention of system compromise is preferable but may not be achievable.

   c. Anonymity of Attacker. Attributing the attack to its ultimate source, if possible, will normally not occur until after the attack has been executed. This limits the range and type of options available to INFOCON decision makers. To effectively operate in this environment, knowledge of the adversary's identity cannot be a prerequisite to execution of defensive strategies and tactics.

   d. Characterization of the Attack. Distinguishing between hacks, attacks, system anomalies, and operator error may be difficult. The most prudent approach is to assume malicious intent until an event is assessed otherwise. See Chapter VII for various assessments to consider.

   e. INFOCON Levels. The NNSA INFOCON system presents a structured, coordinated approach to defend against and react to adversarial attacks on NNSA information, computer systems, and telecommunication networks and systems. The NNSA INFOCON system identifies the five levels of CNA and CNE conditions within NNSA, as shown in Table VIII-1.

Table VIII-1. INFOCON Levels

INFOCON Level	Description
RED (Critical)	Successful information system attack(s) detected that impact NNSA operations such as a Type 1 compromise and/or intrusion or DOS, with a moderate or high impact. Widespread incidents that undermine ability to function effectively. Significant risk of mission failure. Computer Network Attack against national infrastructure or National Security element.
YELLOW (Elevated)	Indications and warnings (I&W) indicate targeting of specific system, location, unit, or operation. Significant level of network probes, scans, or activities detected, indicating a pattern of concentrated reconnaissance. Network penetration or DOS attempted with no impact to NNSA or DOE operations, such as Type 2 attempted intrusion with a low impact. Incident occurs at NNSA site that affects an NNSA Enterprise System, or it may impact another NNSA site, such as a Type 1 compromise and/or intrusion with a low impact. Intelligence indicates imminent attack against NNSA or DOE site.
BLUE (Guarded)	I&W indicate general threat. Regional events occurring that affect U.S .interests and are likely to affect NNSA interests. May involve potential adversaries with suspected or known CNA capability. Information system probes, scans, or other activities detected indicating a pattern of surveillance, such as Type 2 reconnaissance activity with a moderate or high impact. Nation-or Internet-wide computer network exploits, such as a Type 1 Web site defacement, malicious code, or denial of service (DOS), with an impact of low. Increased and/or more predictable threat events. Incident occurs at NNSA or DOE site.
GREEN (Normal)	No significant activity. Normal operations. Network penetration or denial of service attempted with no impact to NNSA, DOE, or site operations such as Type 2 reconnaissance activity or intrusion attempts with a low impact. Minimal attack success, successfully counteracted, such as a Type 1 unauthorized use with a low impact. General threat unpredictable.

4. INFOCON ACTIVITIES.

a. Determining the INFOCON. There are three broad categories of factors that influence the INFOCON: operational, technical, and intelligence, including foreign intelligence and law enforcement intelligence. Some factors may fall into more than one category. The INFOCON level is based on significant changes in one or more of them. Appendix C describes several factors that may be considered when determining the INFOCON. The decision to change the INFOCON should be tempered by the overall operational and security context at that time. For example, an intruder could gain unauthorized access and not cause damage to systems or data. This may only warrant INFOCON BLUE or GREEN during peacetime, but it may warrant INFOCON ORANGE during a crisis. Also, the incident may warrant a high INFOCON at the affected site but not throughout the NNSA as a whole.

b. Declaring INFOCONs. The NNSA CSPM will recommend changes in NNSA INFOCON to the NNSA CIO, who is responsible for declaring an NNSA INFOCON. Assimilation and evaluation of information to assess the CNA and CNE situation NNSA-wide will be a collaborative effort coordinated by the CSPM.

c. Managers of NNSA sites are responsible for assessing the situation and establishing the proper INFOCON, based on evaluation of all relevant factors. See Appendix D and E for criteria and guidance, respectively. NNSA site managers may change the INFOCON of their organizations or site(s); however, they must remain at least as high as the current INFOCON directed by NNSA. Managers changing the INFOCON of their organization or site(s) must report to the CSPM using the same reporting format described in paragraph 4.d of this chapter.

d. Response Measures. Ideally, CNA/CNE operations will be based on advanced warning of an attack. Measures should be commensurate with the risk, the adversary's assessed capability and intent, and mission requirements. Over-aggressive countermeasures may result in self-inflicted degradation of system performance and communication ability, which may contribute to the adversary's objectives. Managers must also consider what impact of imposing a higher INFOCON for their organization will have on connectivity with computer networks and systems of other NNSA sites and operations. Managers will notify the CSPM, through the cognizant ISOM, if recommended or directed response measures conflict with organization or mission priorities. Regardless of the INFOCON level declared at the affected site, it is incumbent upon the affected site to report all unauthorized accesses in a timely manner, in accordance with the NNSA PCSP. Each NNSA site shall have documented procedures to guide their responses and ensure these procedures are well integrated with other site SECON, emergency procedures, and Continuity of Operations plans. See Appendix D and E for recommended action activities.

e. Reporting. Reporting of cyber security incidents must be accomplished as described in Chapter VII. Note, however, that INFOCONs assess potential and/or actual impact to NNSA operations and must be reported as follows:

(1) Reporting Channels. NNSA sites must report INFOCON changes to the NNSA CSPM and the cognizant DAA.

(2) Reporting Frequency. NNSA sites must report INFOCON changes for their sites no later than 4 working hours after the INFOCON has changed. Provide whatever information is available at the time and indicate information that is unknown or unavailable. Information missing from the initial report will be forwarded in a follow-up report within 24 hours of the initial report.

(3) Report Formats. Reports of changes in INFOCON should be accompanied by an operational assessment of the situation, when appropriate. Appendix E outlines a process for assessing the operational impact of a CNA. Report contents shall include, as a minimum:

(a) For all INFOCONs: Organization and location, date and time of report, current INFOCON, reason for declaration of this INFOCON, response actions taken, and POC name and contact information.

(b) INFOCON YELLOW and Higher. All of the above, plus U. S. Computer Emergency Response Team (CERT) or NNSA IARC Number (IARC will report to CIAC) and Law Enforcement Agency (LEA) case number, with POC name and contact information, when available.

(c) INFOCON ORANGE and Higher: All of the above, plus system(s) affected; degree to which operational functions are affected; impact (actual and/or potential) on current and planned missions; and/or general capabilities; restoration priorities; and workarounds.

f. Dissemination of NNSA INFOCON. The CSPM will notify the DAA when the NNSA INFOCON is changed, through the most rapid means available. The DAA sites must notify the CSPM, if recommended or directed INFOCON response measures conflict with organizational or mission priorities, within two (2) hours of NNSA determination of INFOCON response measures. NNSA sites are responsible for rapid dissemination of the INFOCON information within their organization, and to contractor organizations under their cognizance. Notification will include the following information:

(1) Date and time of report.

(2) Current INFOCON.

(3) Reason for declaration of this INFOCON that includes a detailed description of the causal activities and Type and System-Impact Category.

(4) Current and planned operation(s) or capabilities, units and/or organizations, networks, systems, applications, or data assessed to be impacted or at risk.

(5) Recommended or NNSA-directed actions.

(6) References to relevant technical advisories and intelligence assessments

(7) POC information.

(8) Information that may assist sites in their response times. See Appendices D and E.

5. RELATIONSHIP OF INFOCON TO OTHER ALERT SYSTEMS. The INFOCON and SECON may complement each other. The INFOCON may be changed based on the national or global situation, the intelligence community's level of concern, or other factors. Likewise, a change in INFOCON may prompt a corresponding change in other alert systems.

EXERCISES. INFOCON procedures shall be practiced at all NNSA sites as part of their self-assessment program to include operational impact assessments. See Appendix D and E..

CHAPTER IX. PLAN OF ACTIONS AND MILESTONES.

1. INTRODUCTION. This chapter documents the minimum requirements for establishing a management tracking tool for the documentation and correction of security program and system-level findings and incidents. The primary intent of the Plan of Action and Milestones (POA&M) is to assist NNSA management with tracking and mitigating program weaknesses. Additionally, the POA&M assists external regulatory agencies with oversight responsibilities.

   A *finding* is a determined vulnerability pertaining to technology, operations, and/or people that allow compromise to an organization's information or associated information systems. *Findings* are identified through various activities, such as risk management, self assessment, audits, and ST&E processes.

   All NNSA Elements must develop, document, and implement POA&M policies and procedures consistent with the following requirements and commensurate with the level of security required for the organization's environment and specific needs.

   This chapter is compliant with DOE TMR-6, *Plan of Action and Milestones*.

2. CRITERIA AND PROCESSES.

   a. POA&M Content Requirements. Each NNSA Element must define a site-specific POA&M process in their respective CSPPs. The Element's POA&M documentation must include the following information, at a minimum:

      (1) Reporting all program and system-level findings identified by the Office of HSS, the General Accounting Office (GAO), the Office of Inspector General (OIG), and other outside external regulatory agencies. Findings or incidents identified by internal assessment activities, security reviews, or operations are tracked by the POA&M at the determination of the DAA.

      (2) Tracking program and system-level findings with open Corrective Action Plans (CAPs).

      (3) Validating and associated documentation of closure for each POA&M finding.

      (4) Integration of the POA&M process with the internal self-assessment program.

      (5) Identification of the office or organization responsible for tracking and reporting of POA&M information to the NNSA OCIO, on at least a quarterly basis.

(6) Process used to assess POA&M activities on at least a quarterly basis.

(7) Once the POA&M has been reported, changes are allowed to be made to the original description of the finding, key milestones, schedule completion dates, or source under the direction of the DAA. Notations for any modifications to the original entry are to be made separately, and identified as "Changes to Milestones."

(8) POA&M Reports are to be marked and protected as appropriate; at a minimum, reports are to be considered Official Use Only (OUO).

b. Corrective Action Plans. Not all identified findings tracked in the POA&M will have corresponding CAPs. Note, however, that all findings will have associated mitigation milestones tracked within the POA&M. Each NNSA Element must document CAPs at a minimum for any cyber security-related finding identified by the Office of Inspector General and the Office of HSS. If the finding has not been closed within a year of its determination, the NNSA CSPM or cognizant DAA may require that other program or system-level findings be documented in the CAP, based on its impact.

c. CAP Content. For documented cyber-security-related findings, and for program and/or system-level weaknesses that require corrective action plans, CAP must contain, at a minimum, the following content:

(1) A brief overview and summary of the identified weakness, vulnerability, or finding.

(2) Root cause analysis, addressing any systemic program weaknesses.

(3) Mitigation and resolution and recurrence prevention strategies.

(4) Office or organization responsible for remediation.

(5) Resource requirements and expected costs associated with remediation. For system-level POA&Ms, the unique project identifier and project name from the OMB Exhibit 300 or Exhibit 53, where applicable; and for Exhibit 53 systems, the security costs must also be included.

(6) Scheduled start and completion date.

(7) At least one major milestone and estimated completion date.

d. CAP Requirements. In addition to documenting the CAP, as outlined above, the responsible office or organization must also complete the following activities for each CAP.

(1) Risk assessment and acceptance, approval, and communication to impacted organizations and personnel.

(2) Track and update implementation status for each CAP milestone, as directed by the cognizant DAA.

(3) Verify and document the closure of each CAP milestone.

(4) Coordinate the independent validation of milestone completions as directed by the cognizant DAA.

e. POA&M Reports. In accordance with FISMA requirements, NNSA Elements (to include the NNSA HQ Element, must develop, implement, and manage POA&Ms for all cyber security weaknesses and vulnerabilities requiring corrective action, whether or not a CAP has been prepared. POA&M Reports must contain, at a minimum, the following content:

(1) A brief overview and summary of the identified weakness, vulnerability, or finding.

(2) Office or organization responsible for remediation.

(3) Scheduled start and completion date.

(4) At least one major milestone and completion date.

(5) Reported closure of findings and milestones, as validated by someone other than the individual responsible for documenting and tracking the milestones. The POA&M must include the following:

(a) Date of closure.

(b) Finding or milestone closure validated? (Yes or No).

(c) Name, position, and title of validating individual.

(d) Date of validation.

f. POA&M Assessment Requirements.

(1) POA&M-related activities must be tracked, reviewed, and prioritized on at least a quarterly basis. Reviews must include verification that all applicable findings are being tracked and managed.

(2) An assessment of POA&M activities must be conducted when there are changes in organizational roles responsible for POA&M activities; when new Departmental guidance is issued; and/or new findings are identified via an audit, internal review, or self-assessment.

g. Minimum POA&M Reporting Requirements.

(1) POA&M Reports must include program-and system-level findings identified by the Office of HSS, the GAO, the OIG, and other outside external regulatory agencies, as well as any findings and/or weaknesses identified by internal assessment activities or security reviews.

(2) POA&M Reports must include required documentation needed for each system-level finding, such as self-assessments, risk assessments, security plans, certification and accreditation, and contingency plans.

(3) POA&M Reports must include closed findings and milestones for up to one year after formal and validated closure.

(4) NNSA Elements required to report remediation progress on findings and milestones as required by the cognizant DAA, but they are not to report less frequently than quarterly as required by the Office of Management and Budget (OMB).

CHAPTER X. VULNERABILITY MANAGEMENT

1. INTRODUCTION. This chapter establishes the minimum requirements for developing a vulnerability management program, including patch management, for NNSA information systems. Vulnerability management is a measurable, proactive process implemented to secure information systems and to improve regulatory compliance posture. Patch management is one method for addressing vulnerabilities. Note that, because not all vulnerabilities have applicable patches, it is essential that security controls, such as remediations, be implemented based on an analysis of possible vulnerabilities associated with an information system. In addition, such controls help to mitigate the impact of a successful exploitation of an unknown vulnerability. This chapter applies to all NNSA Elements that operate and manage information systems that collect, create, process, transmit, store, and/or disseminate unclassified and classified NNSA information.

2. CRITERIA AND PROCESSES.

   a. Cyber Security Program Plan. Each NNSA Element must address the following vulnerability management program Elements in its site CSPP.

      (1) Vulnerability management activities, including processes for analyzing, detecting, communicating, and remediating vulnerabilities, as well as interfaces to incident management and configuration processes.

      (2) The roles and responsibilities of all key personnel responsible for decisions and activities regarding vulnerability management.

      (3) Awareness, training, and education requirements for all key personnel responsible for vulnerability management activities.

   b. Vulnerability Management Program. Each NNSA Element must implement a vulnerability management program that addresses at a minimum the following requirements:

      (1) Identification, analysis, and dissemination of vulnerability information.

      (2) An inventory of information technology resources, including hardware, operating systems, and software applications, used in the organization.

      (3) Remediation strategies and processes.

      (4) Prioritization of vulnerability remediation or mitigations.

      (5) A standardized vulnerability naming scheme.

      (6) Vulnerability documentation to include POA&M Reports and incident management, as required.

(7) Metrics for testing the effectiveness of the vulnerability management program.

(8) Communication and coordination processes, including internal and external reporting of vulnerabilities and remediation.

(9) A process for identifying, documenting, and communicating lessons-learned regarding vulnerability scanning processes and remediation.

(10) Risk-based standards establishing scan frequency, techniques, and technologies.

(11) A documented vulnerability scanning process that includes the following at a minimum.

(a) Organizational element(s) responsible for conducting vulnerability scanning activities.

(b) Frequency of scanning activities; critical assets and servers must be scanned quarterly.

(c) Identification and prioritization of scanning targets.

(d) Alternate examination methodologies for resources for which operations and production cannot be interrupted.

(e) Identification of resources that cannot be scanned from a central network location.

c. Patch Management Process. Each NNSA operating unit must implement a patch management process that includes at a minimum the following requirements:

(1) Patch prioritization based on criticality of system, network, and specialized tooling.

(2) Testing procedures for patch installation.

(3) Procedures for automated and manual patch deployment.

(4) Identification of those resources that cannot be patched from a central network location.

(5) Patch installation verification processes and methods.

(6) Documentation of residual risk acceptance and integration with CM processes.

(7) Scheduling to ensure that all assets are scanned twice annually, and critical assets and servers are scanned quarterly.

CHAPTER XI. PORTABLE COMPUTING DEVICES

RESERVED – THIS CHAPTER WILL BE DEVELOPED AT A LATER DATE.

This page intentionally left blank.

CHAPTER XII. PASSWORD GENERATION, PROTECTION, AND USE

1. INTRODUCTION. This chapter establishes minimum criteria and processes for the generation, protection, and use of passwords to support authentication when accessing classified and unclassified NNSA information systems, applications, and resources. This chapter applies to any multi-user information system at a NNSA site that collects, stores, transmits, or processes unclassified or classified information, and uses passwords to authenticate users or applications.

2. CRITERIA AND PROCESSES.

   a. Password Generation and Verification. Password generation or verification software must ensure that passwords are generated using the following features:

      (1) Passwords contain at least eight non-blank characters.

      (2) Passwords contain a combination of letters, preferably a mixture of upper and lowercase numbers, and at least one special character within the first seven positions, provided such passwords are allowed by the operating system or application.

      (3) Passwords used on information systems that collect, store, transmit, or process classified information must be machine generated, or use DAA-approved alternative methods of authenticating users or generating passwords.

      (4) Passwords employed by a user on unclassified information systems must be different than passwords employed by the same user on classified information systems.

      (5) Two-factor authentication should be required for all privileged users, accounts, and actions.

   b. Password Protection.

      (1) Passwords used to access information systems processing classified data must be protected at a level commensurate with the classification level and most restrictive category of the information to which they allow access.

      (2) Passwords used to access information systems processing unclassified data must be protected in accordance with the information with the highest impact level for confidentiality or integrity on the system to which they allow access.

(3) Passwords must not:

(a) Contain the User Account Identifier (User ID).

(b) Contain any common English dictionary word, spelled forward or backwards; dictionaries for other languages may also be used if justified by risk and cost benefit analysis, as documented in the approved ISSP or the CSPP.

(c) Employ common names, including the name of any fictional character or place, spelled forward or backwards.

(d) Contain any commonly used numbers, such as the employee serial number, Social Security number, birth date, or telephone number associated with the user of the password.

(e) Contain any simple pattern of letters or numbers, such as “qwertyxx” or “xyz123xx.”

(4) In cases of user-created passwords on unclassified information systems, ensure through verification software and training that selected passwords are consistent with password requirements listed in paragraphs 2a. and b. above.

(5) When an information system cannot prevent a password from being echoed, as in a half-duplex connection, an overprint mask must be printed before the password is entered to conceal the typed password.

(6) Individuals must not:

(a) Share passwords except in emergency circumstances or when there is an overriding operational necessity, as described in the information system's approved ISSP or the site’s CSPP.

(b) Enable applications to retain passwords for subsequent reuse, except as described in the information system's approved ISSP.

(c) Create their passwords if the password is used for access to classified information.

(d) Use group passwords, such as a single password used by a group of users, without some other mechanism that can assure accountability, such as separate and unique network User ID.

(e) Share group passwords outside the group of authorized users. Group passwords must be changed when any individual in the group is no longer authorized to access the information system where the group password is used. Group passwords must ***never*** be reused.

c. Standard Passwords. User software, including operating systems and other security-relevant software, may be supplied with standard identifiers, such as System, Test, and Master, and passwords already enrolled in the system. Passwords for all standard identifiers must be changed before allowing the general user population access to the information system. These passwords must be changed after a new system version is installed or after other action is taken that might result in restoration of these standard passwords.

d. Password Changing. Passwords must be changed:

(1) At least every 6 months.

(2) Immediately, but within one business day, after a password has been shared, compromised, or after the user suspects that a password has been compromised.

(3) On direction from management or the DAA.

e. Administration. The information system, application, or resource where passwords are used for user authentication must, where technically feasible, ensure:

(1) Five consecutive failed attempts to provide a legitimate password for an access request results in an access lockout. The process for restoration of an account must be documented or referenced in the approved ISSP.

(2) The user password, whether user-selected or automatically generated, is rejected if the password does not meet the criteria in this chapter.

(3) Before expiration or lockout will occur, individuals are notified that their passwords are about to expire and must be changed.

(4) Any file, folder, database, or other collection of one or more user passwords is protected from access by unauthorized individuals.

(5) Periodic monthly or quarterly validation of conformance to password policy, as directed by site policy.

f. Clear Text Passwords. The use of clear text passwords must be eliminated from all information systems, applications, and resources.

(1) Each NNSA Element's CSPP shall include a plan, with schedules and milestones, to eliminate the use of clear text, reusable passwords from existing electronic information systems and resources.

(2) Each NNSA Element shall develop procedures to ensure that clear text, reusable passwords are removed from new information systems, applications, and resources before the systems, applications, or resources are placed into production use.

(3) Other mitigation strategies must be in place and must automatically result in a POA&M.

g. Pass-phrase and Entropy-based Passwords. In situations where Pass phrases or entropy-based passwords are used, password generation or verification software must ensure that such passwords meet the following criteria.

h. Pass phrases must contain 25 or more characters and at least 2 special characters, and must not begin or end with a special character.

i. Password generation based on an entropy approach must comply with the guidance for a Level 1 Authentication Mechanism as described in NIST SP 800-63, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*

3. CRITERIA AND PROCESSES FOR PRIVILEGED USERS

a. Privileged Users. Privileged Users are individuals who have access to system control, monitoring, or administration function, such as system administrators, information system security officers, maintainers, and system programmers.

b. Privileged accounts. Privileged accounts are accounts belonging to Privileged Users. Privileged accounts are created for users to perform privileged functions only; that is, privileged users use non-privileged accounts for all non-privileged functions.

The use of mandatory multi-factor authentication process is required for system administrator and privileged user access to systems where passwords are used as one authentication method.

.

CHAPTER XIII. WIRELESS TECHNOLOGIES

1. INTRODUCTION. This chapter establishes the minimum security controls that are to be enforced by NNSA sites using wireless technologies to ensure that security risks posed by wireless applications, devices, and network implementations are analyzed appropriately, and controlled. This chapter applies to any wireless technologies that collect, store, transmit, process, create, or disseminate unclassified or classified NNSA information. In addition, this chapter applies to any wireless technology lifecycle, including development of new wireless applications, incorporation of wireless devices into an infrastructure, incorporation of wireless devices outside the infrastructure, development of prototype wireless technologies, and the reconfiguration or upgrade of existing wireless technologies and legacy systems. Land mobile radios, one-way receive-only devices, and mobile satellite services are excluded from this chapter.

2. CRITERIA AND PROCESSES. In order to ensure that security risks posed by wireless technologies are sufficiently analyzed and appropriately controlled, NNSA sites must establish a systematic process for managing risks posed by wireless technologies, and ensure that the process is described fully in their CSPP. The process must:

   a. Identify the roles and responsibilities of all personnel responsible for the decision whether to incorporate wireless into the environment, including personnel responsible for telecommunications; TEMPEST; Protected Transmission Systems (PTS); and Technical Surveillance Countermeasures (TSCM) program compliance.

   b. Evaluate the business needs for deploying wireless technologies, to include cost-benefit analysis, and whether more secure technologies, such as expansion of the wired network, are feasible.

   c. Include a risk assessment to evaluate risks to the confidentiality, integrity, and availability of site information resources, in the context of exposing information to the hazards associated with utilizing wireless networking devices, and the entire spatial volume through which the transmitted signal is capable of being received. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-48, *Wireless Network Security 802.1, Bluetooth and Handheld Devices*, may be used to assist in decision making.

   d. Ensure that risks for connecting to site LANs are evaluated, and security controls are in place to protect systems and LANs.

   e. Evaluate planned wireless networking applications, with respect to specific wireless technologies, physical location on site, proximity to sensitive or classified information processing areas, connectivity of wireless devices to site computers and networks, and the Information Groups and information systems connected to wireless information systems.

f. Identify specific security mechanisms implemented through technical, operational, management, and assurance controls that will ensure risk is maintained at an acceptable level, and the schedule for testing such controls to ensure they operate as intended. At a minimum, these controls must:

(1) Require semi-annual performance reviews to ensure accuracy of access point inventory, security of configurations, or identification of unauthorized devices.

(2) Require proper installation and physical control of all access points.

(3) Ensure NIC and access-point firmware is up-to-date.

(4) Ensure that only authorized people can reset the access points.

(5) Assign strong passwords to access points. In addition, access points must be administered via the site's wired network, or locally via the access point's built-in COM ports.

(6) Utilize static IP addresses for clients and access points.

(7) Ensure the capability to detect transmissions by unauthorized access points and/or wireless clients is in place and operational before authorized use.

(8) Require the regular application of patches and security enhancements.

(9) Adopt strong encryption methods that encompass end-to-end encryption of information as it passes throughout the wireless network. Use Type II or III products to encrypt transmission of information to or from non-National Security Systems.

(10) Address the DOE TEMPEST/Technical Security Countermeasures (TSCM) concerns, such as wireless, audio, video, and infrared, when allowing operation of these devices in security areas.

g. NNSA Elements utilizing wireless technologies accredited for use with National Security Systems must implement, at a minimum, the following controls:

(1) The wireless device must not be used to download or load any shareware, extraneous software, or unauthorized freeware.

(2) The wireless device must not be synchronized with any unclassified system.

(3) Wireless networks must support security for voice, data, and control channel information, only via approved Type 1 encryption for all modes of operation.

(4) Wireless networks must be monitored to detect unencrypted signals transmitted from areas where classified information is being electronically stored, processed, or transmitted, to ensure that unauthorized signals are not transmitted beyond approved boundaries.

(5) Wireless networks must use security mechanisms compatible and interoperable with those mechanisms used on wired voice and data telecommunication networks and computing devices.

(6) Wireless networks must implement identification and authentication measures at both the device and network level.

This page intentionally left blank.

CHAPTER XIV. REMOTE ACCESS

1. INTRODUCTION. Remote access is defined as accessing an information system, at the system or application level, from a location outside the confines of a network, as defined in each site's CSPP. This chapter does not address risks associated with or criteria and processes specific to wireless networks and devices. Criteria and processes for these are addressed in Chapter XI. Remote access to NNSA information and systems can promote cost-effective benefits to the NNSA mission and workforce. At the same time, remote access can introduce significant risk to those systems. Federal law and implementing policies require agencies to develop, document, and implement programs to assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support agency operations and assets. The remote system used to access a NNSA information system may not have been evaluated through the NNSA PCSP C&A process; therefore, its security policy is unknown. Based upon documented risk assessments, agencies must provide adequate security to maintain an acceptable level of risk to agency operations and assets.

2. CRITERIA AND PROCESSES.

   a. All NNSA sites must develop and implement policies, processes, and procedures to govern remote access of NNSA information systems by users utilizing NNSA and non-NNSA owned equipment. These processes and procedures are documented as part of the site's CSPP. All policies, processes, and procedures must address the following:

      (1) Use of Government- and non-Government-owned computers to access remotely NNSA information resources or information.

      (2) Protection of information on non-Government-owned computers.

      (3) Prohibition by the Department of Commerce of export from the United States of any encryption program or algorithm in excess of 128 bits.

      (4) ISSP modifications, when remote access capabilities are to be introduced into legacy applications or systems.

      (5) Additional security measures required for remote access to SUI, as defined in Appendix B, Glossary.

(6) National Security Systems. Remote access to any DOE and/or NNSA National Security System is authorized via approved methods, such as Type I encryption. The NNSA Element will ensure that only personnel with access authorization and Need-to-Know can access National Security Systems. The risk associated with remote access shall be documented in the relevant ISSP and in the Risk Assessment. Personnel accessing these systems shall be trained, and training shall be documented as required by the ISSP.

(7) Management Controls on Remote Access must describe:

(a) Boundary Protection Services and automated tools, such as firewalls, virtual private networks, encryption, intrusion detection, anti-virus software, audit log analysis provided to manage remote access services and detect intrusions and/or intrusion attempts.

(b) Procedures to report and respond to remote access security incidents.

(c) Rules of behavior and operations and consequences for violating remote access policies and procedures, including prohibition of entering classified information on any computing resource not approved for such information.

(d) Specific security and awareness training for those authorized to use remote access services to access information in all Information Groups, except the Open Public Access Information Group, and those who perform system administration duties.

(e) Process(es) to perform a risk assessment if new threats are introduced by allowing remote access to NNSA information and systems, including trusted and non-trusted environments.

(f) Procedures to ensure that management's initial and periodic approval of operational need of each user's remote access capability is obtained.

(g) Procedures to ensure NNSA systems are protected from malicious code on equipment used for remote access.

(h) Process for organizations and users to obtain approval from system owners and data custodians prior to implementing remote network access.

(i) Processes to ensure that remote access services are controlled, and that user profiles are managed to reflect user job responsibilities.

(j) Processes to ensure periodic reviews and random security evaluations of remote access security controls.

(k) Processes to ensure that remote access issues, vulnerabilities, requirements, and technology changes are incorporated into training for all affected NNSA and contractor personnel, including, as appropriate, the permitted extent of personal use.

(l) Remote access requirements in the ISSP of the system being accessed remotely.

(8) Operational Controls on Remote Access must describe the following:

(a) Minimum requirements for operating systems and application software for users who use non-NNSA owned equipment to connect remotely to NNSA networks, for access to all Information Groups, except the Open Public Access Information Group.

(b) Procedures for obtaining user commitment to the understanding and acknowledgement of minimum requirements and remote access rules of behavior, through user signatures on a User Responsibility Statement that includes requirements for remote access.

(c) Procedures for remote access of NNSA systems from wireless Internet systems in coffee shops, public libraries, or in other such public locations.

(9) Technical Controls. Develop or define and describe the following:

(a) Acceptable levels and types of authentication, and personal identification for remote access.

i. Two-factor authentication, where one of the factors is provided separately from the computer gaining access, such as a RSA token or biometric solution.

ii. Clear-text, reusable passwords for remote access are prohibited. Legacy systems that use clear text passwords are prohibited from participating in remote access.

(b) Establishment of a trusted path prior to transmission of data in all Information Groups except the Open Public Access Information Group.

(c) Time-out function for remote access requiring user re-authentication after user inactivity of 15 minutes for unclassified systems, and 10 minutes for National Security Systems.

(d) Minimum requirements for the operating system and application software and for controlling and safeguarding Government-issued cryptographic keying material on all equipment used for remote access.

(e) Standard minimum security configurations for all information systems.

b. Significant Changes. Owners and operators of interconnected applications and systems must be apprised of any significant change to interconnection agreements. Any site's application or system that uses remote access for which the above criteria are not met must be documented as a weakness in applicable CAPs and POA&Ms.

CHAPTER XV. CONTINGENCY PLANNING

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 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. NNSA recognizes one contingency plan may cover multiple systems, such as one plan that would cover all unclassified desktops.

2. CONTINGENCY PLANNING. The NNSA Contingency Planning Process consists of the following six progressive steps that must be accomplished during the NNSA C&A process.

   a. Site Planning Policy Statement. 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 for activating the contingency plan(s). 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). The site shall conduct BIAs to identify systems that provide 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 (CPC) to fully characterize 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) A BIA for any system designated a Critical Infrastructure or Key Resource may be limited to a determination of critical components required 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.

(4) Identify data on the systems and specify protection measures of the data based on level of confidentiality or classification, such as encryption of backups or secure storage.

(5) Identify data users, providers, and flows.

(6) Identify system components and infrastructure, such as electric power, servers, routers, authentication servers, required to extract or enter data.

(7) Identify disruption impacts and allowable outage times.

(8) Identify 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.

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

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

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

(12) Develop recovery priorities.

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

(14) Determine recovery timeline for each system component.

(15) Initiate preparation of POA&Ms for any systems that are prioritized below current funding capabilities.

c. Preventive Controls. 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 POA&Ms as necessary for any system that is prioritized below current funding capabilities.

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

(1) Identify 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) Note that 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) Management

(b) Damage Assessment

(c) Alternate Site Recovery and Coordination

(d) Hardware Salvage

(e) Data Recovery

(f) Database Recovery

(g) Application Recovery

(h) LAN and/or WAN Recovery

(i) Telecommunications

(j) Network Operations Recovery

(k) Software and Data Recovery

(l) System Software

(m) Operating System Administration

(n) System Recovery

(o) Server Recovery

(p) Administrative Support

(q) Original Site Restoration and Salvage Coordination

(r) Test

(s) Procurement (equipment and supplies)

(t) Physical and Personnel Security

(u) Transportation and Relocation

(v) Media Relations

(w) Legal Affairs

(4) Update the POA&M as necessary to include resource requirements to implement this portion of the CP.

e. Testing, Training, and Exercises. Testing the plan identifies planning gaps. 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 a CP involves the definition of a scenario, test objectives, and criteria that must be met to successfully complete the test of each CP element.

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

(3) Test reports for Critical Infrastructure and Key Resources must be forwarded to the Office of the NNSA CIO through the SOM or SCD, as applicable.

(4) Testing may take four forms, as follows:

(a) Structured Walkthrough. The most basic type of test. A Structured Walkthrough takes place in a group meeting type of setting, where the main goal is to confirm that critical personnel from all areas are familiar with the BCP – provides an orientation. This test does not usually involve the entire organization, nor does it test the team's ability to execute it.

(b) 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. At a minimum, a Tabletop Exercise of CPs for all systems must be conducted annually, when a Functional Exercise is not conducted.

(c) Functional Exercise. This takes place in a simulated environment and utilizes physical testing of procedures, alternate equipment, and alternate locations, to ensure the correctness of procedures, capability of recovery personnel, and technical capabilities of equipment. A Functional Exercise of Critical Infrastructure and Key Resource CP must be conducted annually. All Moderate and High category information systems should undergo a Functional Exercise at least every 2 years to include elements of Notification and Activation, Recovery, and Reconstitution, as a minimum.

(d) Full-Scale Exercise. The most comprehensive test is the Full-Scale Exercise, also known as the Operational Exercise. During this test, all or most of the BCP is put into action. The main goal is to simulate an actual recovery situation as closely as possible. The exercise will evolve and develop just as they would in an actual crisis.

(5) Training. Recovery personnel must be trained to understand the CP and their applicable role. This training will be accomplished annually and as part of changes to the CP. 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 and activation, recovery, and reconstitution.

(f) Individual responsibilities in contingency processes.

(6) POA&M Update. Update the POA&M as necessary, to include resource requirements to implement this portion of the CP.

f. Plan Maintenance. The plan is a living document that is reviewed and updated annually to remain current with system enhancements, results of plan testing, team staffing changes, and changes in NNSA priorities.

The CP shall be a configuration item and maintained as part of the ISSP. A change to the system or its environment, which includes CP elements, requires the modified ISSP to be approved prior to implementing the changes.

3. CONTINGENCY PLAN DEVELOPMENT. The CP contains detailed roles, responsibilities, teams, and procedures associated with restoring an IT system following a disruption. The CP should document technical capabilities designed to support contingency operations and be tailored to the site and its requirements. A site-level CP may be written to describe processes that are common to all CPs, 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.

a. Introduction. The Introduction includes background and contextual information that makes the 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 subparagraph establishes the reason for writing the plan.

(2) Applicability. The organization(s) impacted by the CP 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 paragraph discusses the issues, situations, and conditions addressed and not addressed in the CP. 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.

c. References and Requirements. This subparagraph identifies the NNSA, Program, and site requirements for contingency planning.

d. Record of Changes. This subparagraph describes the configuration history of the CP by recording dates, version, and reason for CP changes.

e. Concept of Operations. The Concept of Operations (CONOPS) element provides additional details about the system, planning framework, response activities, recovery activities, and resumption activities.

f. System Description. The system description should include system architecture, location(s), internal and external connections, security components, and any other technical detail that would assist contingency teams in understanding the system configuration and operation.

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

(2) Responsibilities. This subparagraph describes the overall structure of the contingency teams. Coordination mechanisms and requirements, as well as an overview of team member roles and responsibilities are also described.

g. Notification and Activation. The Notification and 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.

h. 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, telephone 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 POCs are identified in the ISSP Memorandum of Agreement (MOA)/System Interconnect (SIA) Agreement, but should also be listed in the CP for ease of use when needed.

i. Damage Assessment. In order to appropriately implement the CP, 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, such as structural integrity of the building or room, electric power availability, HVAC, and telecommunications.

(5) Inventory and functional status of system components.

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

(7) System components to be replaced.

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

j. Plan Activation. The CPC 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 paragraph of the plan, and it 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.

k. Recovery. The Recovery element includes the operations that begin after the CP 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. Upon completion of the Recovery Phase, the system will be operational and performing the functions designated in the plan.

l. Recovery Sequence. The sequence of recovery 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 that 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. 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 when items must be procured.

m. 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 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).

(10) Operating alternate equipment.

n. Reconstitution. Once the original or new site or 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 and/or facility. Until the primary system is restored and tested, the alternate system should continue to be operated.

o. The CP 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) Establishing connectivity and interfaces with network components and external systems.

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

(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 alternate system.

(7) Terminating contingency operations.

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

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

4. CONTINGENCY PLAN STRUCTURE. The structure of a CP is based on the importance of systems for which the plan is written. The following paragraphs describe the mandatory CP elements based on the designation of the system. Refer to Appendix G, Contingency Plan Structure.

a. Critical Infrastructure. Critical Infrastructure CPs must address each of the elements described in 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 Resource CPs must address each of the elements indicated in the following paragraph in sufficient detail for personnel familiar with the system to create and operate the system in a different location.

(1) Introduction (3.a)

(2) Scope (3.b)

(3) Concept of Operations (3.c)

(4) Notification and Activation (3.d)

(5) Recovery Procedures (3.e)

(6) Reconstitution (3.f)

c. Remaining Systems. All other system CPs must address each of the elements, as indicated in the paragraphs 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 (3.c.)

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

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

(6) Notification and Activation

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

(8) Plan Activation (3.d.(3))

(9) Recovery Procedures

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

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

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

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

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

(15) Operating Equipment (3.e.(2)(j)

(16) Reconstitution

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

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

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

This page intentionally left blank.

CHAPTER XVI. CLEARING, PURGING, AND DESTROYING MEDIA

1. INTRODUCTION. This chapter establishes NNSA policy requirements and responsibilities for clearing, purging, and destroying NNSA information system storage media, memory devices, and other related hardware, hereafter referred to as storage media. Specifically, this chapter provides the following:

   a. Instructions for clearing, purging, and destroying storage media to preserve the confidentiality of the stored information.

   b. Instructions for handling classified storage media that will be reused in controlled environments.

   c. Instructions for sanitizing storage media that has become contaminated with classified or unclassified sensitive information.

   d. Direction to ensure that no unauthorized information can be retrieved from unclassified NNSA and DOE computer equipment, and storage media that is to be transferred or declared surplus.

   e. Direction to ensure that all NNSA Element personnel are made aware of requirements for clearing, purging, and destroying information system storage media, memory devices, and related hardware.

2. CRITERIA AND PROCESSES.

   a. Approved Processes. NNSA-approved processes for clearing, purging, and destroying information system storage media, memory devices, and related hardware that have been used to process, store, or contain unclassified or classified information are listed in the following paragraphs. Decisions to clear, purge, or destroy information system storage media, memory, and other related hardware must be based on the confidentiality of the most sensitive information ever recorded on the storage media. Implementation of these processes and plans for clearing, purging, and destroying information system storage media must be documented in the appropriate CSPPs, including the requirement for documented methods for independently verifying the clearing and purging results.

   b. CSPP. The CSPP must identify or reference procedures used for the sanitization (clearing, purging, and destruction) that implement the concepts and processes listed below.

      (1) Maintenance on equipment and tools used for clearing, purging, and destruction is regularly scheduled and performed to ensure proper operation and calibration.

      (2) All maintenance on equipment and tools used for clearing, purging, and destruction are thoroughly documented.

(3) Systems media and storage hardware are purged before release to personnel without authorization to access the information, including Need-to-Know, on the media or hardware.

(4) Processes for handling and control of media, electronic devices, and hardware prior to clearing, purging, or destruction are documented and followed.

(5) Storage media used in SUI processing is tracked and controlled until it is purged or destroyed.

(6) The storage media must be tracked and destroyed if the confidentiality impact is moderate or high, unclassified information is located in bad sectors, or the storage media cannot be cleared or purged.

(7) Storage media that has been used in classified processing and is no longer being used or needed for archiving is tracked and controlled until it is destroyed, and the destruction is documented as required by the DOE Classified Matter Protection and Control (CMPC) program.

(8) Sanitization procedures, software, equipment and tools, and special processes are identified, documented and approved by the DAA.

(9) Decision and handling processes regarding reuse of classified storage media at lower classification level(s) include formal risk and cost analyses and testing and are documented and justified.

(10) Requirements for removing information from storage media, memory devices, and related hardware are to be included in the training and awareness program and reviewed with all users on a regular basis.

(11) Personnel performing or verifying clearing, purging, or destruction of storage media, memory devices, and other hardware are to be trained in equipment and tool operation, approved techniques, and procedures.

(12) No fewer than 20 percent of the purged media are sampled on a controlled, random basis to verify the purging process has been successfully completed.

(13) Verification is conducted by individuals other than those performing the purging processes**.**

(14) The completion and verification of the purging process is documented.

c. Minimum Sanitization Criteria. Table XVII-1 through Table XVII-3 outline the basic sanitization processes and tools based on different technologies and media types.

(1) NSA/CSS Manual 9-12/20 or subsequent update may be used as a supplement for these processes.

(2) NIST SP 800-88, *Guidelines for Media Sanitization*, or subsequent update may be used as a supplement for these processes.

(3) Refer technologies and media types not listed in the tables or references through the NNSA CSPM to DOE OCIO for defining clearing, purging, and destroying processes.

d. Unclassified Storage Media Processes.

(1) In addition to the clearing processes listed in Tables XVI-1 through XVI-3, processes to clear unclassified storage media are to include the following:

(2) Storage media hosting Government information is to be cleared if it will be reused by a potential user who has a different authority for access, including Need-to-Know, or in a system that contains information whose Security Category (confidentiality, impact) is the same or higher.

(3) Only overwriting software and hardware that are compatible with media to be overwritten and approved by the DAA will be used. Care should be used to ensure a match of software and hardware to the media, considering the make, model, and manufacturing date of the media.

(4) One-pass overwrites are sufficient for clearing storage media that does not contain SUI. If the storage media contains SUI, three-pass overwrites must be performed.

(5) Individuals performing unclassified storage media clearing must certify and document successful completion of the process to include the following:

(a) Purpose of clearing (reuse or release).

(b) Storage media unique identifiers, such as serial number, make, and model.

(c) The Information Type with the highest confidentiality impact hosted on the media prior to clearing.

(d) The procedure used.

(e) The date, the printed name, and signature of the certifying individual.

(6) All unclassified storage media will not be released to the public.

(7) Individuals performing unclassified storage media purging must certify that the purging process has been successfully completed by affixing a label to the storage media. At a minimum, the label must document the following:

(a) Storage media unique identifiers, such as serial number, make, and model.

(b) The Information Type with the highest confidentiality impact hosted on the storage media prior to purging.

(c) Purpose of purging.

(d) The procedure used.

(e) The date, printed name, and signature of the certifying individual.

(f) Storage media that cannot be purged must be destroyed.

e. Classified Storage Media Processes.

(1) In addition to the clearing processes listed in Tables XVI-1 through Table XVI-3, processes to clear classified storage media must include the following:

(2) Storage media that will be reused on a different system for the same or more restrictive Information Group or a potential user has a different Need-to-Know must be cleared.

(3) Only overwriting software and hardware that are compatible with media to be overwritten and approved by the DAA will be used.

(4) Cleared storage media that has been used in classified processing must be protected commensurate with the highest Information Group it has ever contained. The media must be handled in accordance with applicable DOE Classified Matter Protection and Control processes.

(5) Individuals involved in clearing classified storage media must certify and document the successful completion of the process to include:

(a) Storage media unique identifiers, such as serial number, make, and model, and ACREM accountability number.

(b) Most restrictive Information Group hosted prior to clearing.

(c) Purpose for clearing.

(d) The procedure used.

(e) The date, the printed name, and the signature of the certifying individual.

(6) In addition to the purging processes listed in Tables XVI-1 through XVI-3, processes to purge classified storage media are to include the following.

(a) Classified storage media that cannot be reused at a lower level must be destroyed.

(b) Classified storage media that has been purged may not be donated, sold, or released from the DOE environment to outside organizations.

(c) Individuals performing purging of classified storage media must certify the process has been successfully completed by affixing a label to the storage media. At a minimum, the label must document the following:

(i) Storage media unique identifiers, such as serial number, make, and model.

(ii) Most restrictive Information Group hosted prior to purging.

(iii) Purpose of purging.

(iv) A statement that the storage media contains no classified information.

(v) The procedure used.

(vi) The date, printed name, and signature of the certifying individual.

f. Special Circumstances. The use of storage media in a lower classification is described below.

(1) Reusing Classified Storage Media.

(a) The decision to reuse storage media at a lower classification level may be acceptable if formal risk and cost analyses are conducted, and the results of these analyses and testing of the implemented procedures verify that the National Security of the United States is not adversely affected. Testing, risk and cost analysis procedures must be documented in the site's approved CSPP.

(b) Reuse of storage media must be identified in the ISSP of the system where the media is used and the media must be tracked and controlled until it is purged or destroyed.

(c) Classified storage media that will not be reused at a lower classified level must be destroyed.

(d) The storage media must be purged by overwriting the entire storage media using the three-pass process described in Table XVI-1 of this document.

(e) The software used is to provide information about sectors overwritten and bad sectors that cannot be overwritten.

(f) Quality controls are to be documented and deployed for review of overwrite process results and verification that all the classified information was completely overwritten

(g) Storage media must be destroyed if classified information is located in bad sectors or the storage media cannot be purged.

(h) Individuals performing purging of the classified storage media planned for reuse must certify the process has been successfully completed by affixing a label to the storage media. At a minimum, the label must document the following:

(i) Storage media unique identifiers, such as serial number, make, and model, and ACREM accountability number.

(ii) Most restrictive Information Group hosted prior to purging.

(iii) Purpose of purging.

(iv) A statement that the storage media contains no classified information.

(v) The procedure used.

(vi) The date, printed name, and signature of the CA.

(2) Purging Partially Contaminated Storage Media. Areas of non-removable and removable storage media partially contaminated with an information type of a higher confidentiality impact or more restrictive Information Group may be purged using the three-pass process described in Table XVI-1 and continue use in its current information system in the following situations:

(a) When the classified storage media is contaminated with relatively small amounts of information from a more restrictive Information Group (less than 0.1 percent of the capacity of the non-removable storage media).

(b) When unclassified storage media is contaminated with relatively small amounts of unclassified information with a confidentiality

impact of moderate or high (non-Public) (less than 0.1 percent of the capacity of the non-removable storage media).

(c) The software used to overwrite contaminated storage media must overwrite all contaminated locations, including temporary data file locations, file slack, free space, and directories; provide confirmation of overwrite of specified areas and of successful completion; and provide information about sectors overwritten and bad sectors that cannot be overwritten.

(d) Quality controls are to be documented and deployed for review of overwrite process results and verification that all the contaminating information was completely overwritten.

(e) Storage media must be destroyed if classified information is located in bad sectors, or the storage media cannot be purged.

(f) Records to be maintained, as a minimum, are listed below.

(i) Storage media unique identifiers, such as serial number, make, and model.

(ii) Contaminating Information Group.

(iii) Purpose of purging.

(iv) A statement that the storage media no longer contains the Information Group.

(v) The procedure used.

(vi) The date, printed name, and signature of the certifying individual.

Table XVII-1 shows the approved processes for clearing, purging, and destroying storage media.

Table XVI-1. Approved Processes for Managing Storage Media

Media Type	Clearing‡	Purging‡	Destroying‡
Magnetic Tapes			

Media Type	Clearing‡	Purging‡	Destroying‡
Type I	1, 2, or 3	1, 2, 3, or 4	5
Type II	1, 2, or 3	2, 3, or 4	5
Type III	2 or 3	3 or 4	5
Magnetic Disks			
Floppies, Zip drives	1, 2, 3, or 4	X	5
Bernoulli Boxes	1, 2, 3, or 4	X	5
Removable Hard Disks	1, 2, 3, or 4	1, 2, 3, or 4	5 or 6
Non-removable Hard Disks	4	1, 2, 3, or 4	5 or 6
Optical Disks			
Magneto-optical: Read Only	X	X	4
Write Once, Read Many (WORM)	X	X	4
Read Many, Write Many	X	X	4
Other			
Floptical	X	X	5
Helical-scan Tapes	X	X	5
Cartridges	X	X	5
Optical	X	X	5
CD-R, -RW, -ROM	X	X	5 or 7
DVD	X	X	5 or 7

‡ Numbers in the table refer to the processes listed.

§ All degaussing products used to clear or sanitize media must be certified by the National Security Agency (NSA), and be listed on the Degausser Products List of the NSA Information Systems Security Products and Services Catalogue.

Processes: †

Degauss with a Type 1 degausser.§

1. Degauss with a Type 2 degausser.§
2. Degauss with a Type 3 degausser.§
3. Overwrite all locations with a pseudorandom pattern twice and then with a known pattern.
4. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure media are physically destroyed.
5. Remove the entire recording surfaces by sanding or applying acid.
6. Grind surface of CD or DVD to ensure the entire recording surface is removed. Only NSA Group D equipment and associated processes approved for the specific media may be used.

X. No process authorized.

Table XVII-2 illustrates the approved processes for clearing, purging, and destroying electronic memory devices.

Table XVI-2. Approved Processes for Managing Electronic Memory Devices

Media Type	Clearing‡	Purging‡	Destroying‡
Magnetic Bubble Memory	2	1 or 2	10
Magnetic Core Memory	2	1 or 2	10
Magnetic Plated Wire	2	2 and 3	10
Magnetic-Resistive Memory	2	X	10
Read-Only Memory (ROM)	X	X	10 (see 11)
Random Access Memory (RAM) (Volatile)	2 or 4	4, then 9	10
Programmable ROM (PROM)	X	X	10
Erasable PROM (UV PROM)	6	6, then 2 and 9	10
Electrically Alterable PROM (EAPROM)	8	7, then 2 and 9	10
Electrically Erasable PROM (EEPROM)	2	8, then 2 and 9	10
Flash Erasable PROM (FEPROM)	8	8, then 2 and 9	10

‡Numbers in the table refer to the processes listed.

§ All degaussing products used to clear or sanitize media must be certified by the National Security Agency (NSA) and be listed on the Degausser Products List of the NSA Information Systems Security Products and Services Catalogue.

Processes: ‡

1. Degauss with a NSA approved Type III degausser.§
2. Overwrite all locations with a pseudorandom pattern twice and then with a known pattern.
3. Purging is not authorized if data resided in same location for more than 72 hours; sanitization is not complete until each overwrite has resided in memory for a period longer than the classified data resided in memory.
4. Remove all power, including batteries and capacitor power supplies, from RAM circuit board.
5. Perform an ultraviolet erase according to manufacturer's recommendation.
6. Perform an ultraviolet erase according to manufacturer's recommendation, but increase time requirements by a factor of 3.
7. Pulse all gates.
8. Perform a full chip purge/ erase (see manufacturer's data sheet for procedure).
9. Check with ISSO to determine whether additional processes are required.
10. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure media are physically destroyed.
11. Destruction required only if ROM contained a classified algorithm or classified data.

X. No process authorized.

Table XVII-3 shows the approved processes for clearing, purging, or destroying hardware.

Table XVI-3. Approved Processes for Managing Hardware

Media Type	Clearing‡	Purging‡	Destroying‡

Media Type	Clearing‡	Purging‡	Destroying‡
Printer Ribbons	6	6	6
Platens	X	1	6
Toner Cartridges	5	5	X
Laser Drums	3	3	6
Cathode-Ray Tubes (If there is Classified Burn-In)	X	6	6
Fax Machines	4	4	6
Cell Phones	7	X	6
Personal Digital Assistant (PDA) (Palm, Pocket PC, etc.)	7	X	6
Routers/Copy machines	7	X	6
All other storage media devices	X	X	6

‡Numbers in the table refer to the processes listed.

Processes:

†

1. Chemically clean so no visible trace of data remains.
2. Print at least five pages of randomly generated unclassified data. The pages should not include any blank spaces or solid black areas.
3. Print three blank copies. If unable to get a clean output, print an unclassified test pattern or black copy; then run three blank copies.
4. For fax machines that have memory and other storage media incorporated, treat each component per processes listed in tables 1 and 2 of this chapter.
5. Upon completion of copying or facsimile processing of classified material, users are required to run ten (10) blank copies to ensure the removal of all classified materials from processing device.
6. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure the media is physically destroyed.
7. Manually delete all information, then perform a full manufacturers reset to reset the instrument back to factory default settings.

X. Not applicable.

Note: All copies printed for clearing and sanitization purposes must be destroyed as classified waste.

CHAPTER XVII. SENSITIVE UNCLASSIFIED INFORMATION

1. INTRODUCTION. This chapter describes the terms Sensitive Unclassified Information (SUI), including Personally Identifiable Information (PII) as defined by DOE. NAP 14.2-C, NNSA Certification and Accreditation (C&A) Process, establishes the minimum security criteria and processes for protecting this type of information. All NNSA Elements must develop, document, and implement policies for protecting SUI, including PII.

2. CRITERIA AND PROCESSES. To ensure that SUI, including PII, on NNSA information systems is appropriately managed, each NNSA site must establish policies and procedures that address the following:

   a. Sensitive Unclassified Information. SUI is defined as unclassified information requiring protection mandated by policy or laws, such as OUO; Export Control Information (ECI); Unclassified Controlled Nuclear Information (UCNI); Naval Nuclear Power Information (NNPI); Personally Identifiable Information (PII); and other information specifically designated as requiring SUI protection. Extensions of the definition of SUI must be documented in the Element's CSPP and ISSP.

   The OMB definition of PII is included below. This definition is not to be modified by Senior DOE Management or its elements. Senior DOE Management should interpret this definition by applying the working examples of what is and what is not considered PII, provided in Appendix B, to identify PII within their organizations.

   b. Personally Identifiable Information (PII) (as defined by OMB)**.** Personally Identifiable Information (PII) is any information about an individual maintained by an Agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security numbers, date and place of birth, mother's maiden name, biometric records, including any other personal information that is linked or linkable to an individual. In some instances, PII overlaps with Privacy Act information.

This page intentionally left blank.

CHAPTER XVIII. PEER-TO-PEER (P2P) NETWORKING

1. INTRODUCTION. Peer-to-peer (P2P) technology, services, and applications are useful but introduce significant risks that must be mitigated to maintain the security of DOE systems and networks. All NNSA Elements must use a risk-based approach when evaluating the possible use of P2P technologies, as well as address the following minimum security requirements.

2. CRITERIA AND PROCESSES. NNSA Elements must develop and implement risk-based policies and procedures that govern the consideration and possible implementation of P2P technologies in accordance with the following security criteria:

   a. The default condition is that P2P applications, technology, or services are not to be used on DOE systems that contain or process SUI.

   b. P2P applications are prohibited from being employed in any National Security System.

   c. If the application of P2P technology or service is required to meet programmatic or mission requirements, then each application of the technology must be justified and approved by the DAA during the C&A process. At a minimum, the justification must include:

      (1) Description of the P2P protocol(s) and application(s).

      (2) Risk assessments for systems where P2P technology or services are to be used.

      (3) Identification of controls at the system and network levels to detect improper use and attempted evasion of security controls.

   d. If a NNSA Element does implement P2P technology based on a DAA-approved justification, the following management and technical security controls (at a minimum) are to be addressed and implemented for applications, system components, and networks that are part of, or may come in contact with, P2P technologies or services. Implemented controls are to be documented and tested in all associated ISSPs during the C&A process.

      (1) Technical controls that do not allow the P2P server-client applications to automatically reply (Pongs) to broadcasts for locating another server-client (Pings).

      (2) Management controls describing the rules of behavior for users.

(3) Protocols specific to P2P server-client applications are not passed between systems or on the network unless specifically authorized in an ISA for each system hosting a P2P server-client application.

(4) Firewall rules and access control lists (ACL) must be specifically established to allow, should be restrictive to specific systems, and be appropriately documented.

(5) Technical controls that provide the capability for boundary protection services to detect and block unauthorized P2P applications, services, and software ports.

(6) Need-to-Know and access authorizations are enforced and implemented as required for the Information Groups and security categorization of the affected system.

(7) Technical controls that limit operation of a server-client application to downloading (pull), and that does not accept remote writing to the system disk hosting the P2P application from another system or system component (push).

(8) Technical controls that limit ports authorized for use be P2P applications. P2P is denied/disabled on all systems and must be specifically approved to be enabled.

CHAPTER XIX. FOREIGN NATIONAL ACCESS

1. INTRODUCTION. This chapter establishes the requirements for defining Foreign National Access to NNSA information and the information systems that contain such information. Information systems include, but are not limited to, computers, networks, associated servers, data storage devices, and portable and mobile devices. A process for defining Foreign National Access to NNSA information systems is needed to enforce access restrictions based on Need-to-Know, therefore providing adequate protection to information assets. All NNSA Elements must develop, document, and implement policies pertaining to information system access by Foreign Nationals, as dictated by the following criteria. Further, such policies must be commensurate with the level of security required for the organization's environment and specific needs.

2. CRITERIA AND PROCESSES. To ensure that Foreign National Access to NNSA information systems is managed appropriately in an effort to reduce the risk of unauthorized access to information assets, each NNSA Element must establish policies and procedures that include the following criteria, at a minimum.

   a. Roles and responsibilities of personnel involved in approving, implementing, and monitoring Foreign National Access to NNSA information systems.

   b. Specific requirements for approval, documentation, and review of Foreign National Access to information systems as required by DOE O 142.3, *Unclassified Foreign Visits and Assignments*, and DOE O 142.1, *Classified Visits Involving Foreign Nationals.*

   c. Access to National Security systems by Foreign Nationals must include an access approval by the system owner via the processes detailed in DOE O 142.1.

   d. Policies specifying the use, or prohibition, of Foreign National-owned computing equipment connected to NNSA information systems. Such equipment includes computer systems, external computing devices, and electronic media.

   e. Policies describing the screening process for Foreign National Access to NNSA information systems dependent on the security category of the information system, the information type, and the level of access required by the Foreign National, such as general user, privileged user, or System Administrator.

f. Access to SUI systems by Foreign Nationals must include the following:

(1) If a general user, a background screening that includes a Human Resources Background Check and a National Agency Check.

(2) If a privileged user, a background screening that includes a Human Resources Background Check and a National Agency Check with Inquiries.

(3) Processes for monitoring and evaluating the effectiveness of Foreign National Access policies and procedures.

(4) Policies prohibiting Foreign National use of non-DOE equipment to access National Security systems.

3. CYBER SECURITY PROGRAM PLANS. Each NNSA Element must document policies for allowing Foreign National Access to NNSA information systems consistent with the following criteria in their site CSPP.

a. Access to information systems by Foreign Nationals must be approved and documented.

b. Approval documentation must identify the applicable security plan, as required by DOE O 142.1 and/or DOE O 142.3, the information and information systems(s) to which access is granted, and the time period of access.

c. The official accountable for the access approval decision is to be identified in the documentation.

d. Access is granted based on a documented risk assessment and identification of access controls.

e. The approved risk assessment must be referenced in the security plan, and the specific information system access controls must be documented in the security plan.

f. The risk assessment must address certain security factors, such as type of security area where work will be accomplished or visited, sensitivity of all information accessible during the work or visit, and Foreign National affiliation with sensitive countries or countries identified as state sponsors of terrorism. In addition, the risk assessment must address the results of subject matter expert (SME) reviews as required by DOE O 142.3.

g. Procedures for reviewing and managing Foreign National Access to NNSA information systems must be documented. The procedures must include:

(1) Documenting, monitoring, and tracking Foreign National Access to NNSA information systems.

(2) Auditing Foreign National Access to NNSA information systems consistent with the documented risk assessment.

(3) Security incident reporting and resolution involving Foreign National Access.

(4) Training for approval authorities and Foreign National sponsors or supervisors as described in DOE O 142.1 and DOE O 142.3.

(5) Policies prohibiting the use of encryption software provided by foreign governments.

This page intentionally left blank.

CHAPTER XX. NNSA INTER-SITE NETWORK INTERCONNECTION APPROVAL PROCESS, APPROVAL AUTHORITY, AND CONNECTION REQUIREMENTS

1. INTRODUCTION. The purpose of this NNSA Inter-site Network Interconnection Approval Process and Connection Requirements document is to establish the connection approval process, approval authority, and connection requirements for all of the NNSA inter-site connections, including: (1) "site to Enterprise," (2) "site to site," (3) "site to non-NNSA."

2. OBJECTIVES.

   a. The objectives are to ensure that:

      (1) All inter-site connections are compliant with established directives and guidance; meet all technical and interoperability requirements.

      (2) Operational requirements have been met and validated; sub networks, systems, and other connected components.

      (3) Sub networks, systems, and other connected components:

         (a) Provide adequate security.

         (b) Have been accredited by the proper authority; and connection requirements are established, and site compliance validation visits are performed.

      (4) Connection requirements are established, and site compliance validation visits are performed.

3. REQUIREMENTS. All inter-site network interconnections must meet the following mandatory requirements for an authority to connect to be granted.

   a. Authority to Operate (ATO) or Interim Authority to Operate (IATO). Each information system connected to an NNSA site will have been granted an ATO or IATO by the associated Federal DAA. Each NNSA DAA that is responsible for a network interconnection will verify that a current ATO or IATO acceptance letter exists for each network and related systems included and impacted by the interconnection. Where appropriate, the DAA may also choose to review the system ISSP.

   b. Interconnection Security Agreement. Every NNSA Inter-site network connection that involves networks and systems supported by a different DAA requires an ISA. Each DAA that is responsible for a network interconnection involving an NNSA site will review and sign the ISA, which documents technical security specifications for the interconnection between connecting systems. The ISA must

include, or refer to an external document such as the ISSP that includes, the following:

c. Interconnection Statement of Requirements.

(1) Business requirement for the interconnection as well as a reference to the risk analysis conducted to justify the interconnection.

(2) Names of the systems being connected and personnel points of contact for the interconnected systems, including the cognizant DAAs.

(3) Reference to MOU associated with ISA.

d. System Security Considerations.

(1) General Information and Data Description. A description of the information and data that will be made available, exchanged, or passed one-way only by the interconnection of the two systems.

(2) Services Offered. The nature of the information services, such as e-mail, file transfer protocol (FTP), database query, file query, or general computational services offered over the interconnection by each organization must be described and include network ports, protocols, direction of data flow, services being utilized.

(3) Data Sensitivity. The sensitivity level of the information that will be handled through the interconnection, including the highest level of sensitivity involved, and the most restrictive protection measures required, must be explicitly defined.

(4) User Community. A description of the users that will be served by the interconnection, including their approved access levels and the lowest approval level of any individual who will have access to the interconnection, must be described. The description must include any applicable requirements for background investigations and security clearances, and what access is permitted by foreign nationals.

(5) Information Exchange Security. A description of all system security technical services pertinent to the secure exchange of data between the connected systems must be documented to include the method for authenticating the legitimacy of the requesting system.

(6) Trusted Behavior Expectations. A summary of the aspects of behavior expected from users who will have access to the interconnection must be documented. Each system is expected to protect information belonging to the other through the implementation of security controls that protect against intrusion, tampering, and viruses, among others.

(7) Telecommunication Channel. A description of the telecommunications channel and requirements surrounding the connection must be outlined, including information about whether the connection traverses a public network and what vendor is supporting the solution.

(8) Enclave Protection. Protection mechanisms for each network should be described, to include the implementation of controlled interfaces, firewalls, and Intrusion Detection Systems (IDS).

(9) Compliance Deviations. All NNSA deviations from NNSA security requirements will be documented for each network involved in the inter-site network connection.

(10) Configuration Management. The responsibilities and processes for mutual management, maintenance, operation, and configuration maintenance for the interconnection must be documented.

e. Topological Drawing. A topological drawing must be included that provide the following elements:

(1) Defines the system's boundaries.

(2) Includes communications paths, circuits, and other components used for the interconnection.

(3) Depicts the logical location of all components, such as firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations, including IP addresses.

(4) Depicts all other network connections, including remote access services.

(5) Is marked at the top and bottom of each page with an appropriate handling requirement, minimally "Official Use Only."

f. Signatory Authority.

(1) Expiration date of the agreement.

(2) Periodic review requirements. The requirements for periodic review of the agreement must be explicitly stated. The stated review period must be at least annual.

(3) Signatures of the applicable DAA for each system and network participating in the interconnection.

(4) Memorandum of Understanding. For interconnections that involve two or more DAAs, an MOU must be developed that defines the responsibilities

of the participating organizations and individuals. Additionally, the MOU defines the purpose of the interconnection, identifies relevant authorities, specifies the responsibilities of both organizations, and defines the terms of agreement and the timeline for terminating or reauthorizing the interconnection. Each NNSA DAA responsible for a participating system and network connection must review and sign the MOU. Refer to Appendix I for a sample MOU.

g. Security. Both parties must agree to abide by the security arrangements specified in the ISA. In addition, state that both parties certify that their respective system is designed, managed, and operated in compliance with all relevant Federal laws, regulations, and policies. Each DAA must agree to inform the other affected DAA about any changes to the security posture of the network, including the addition of new network connections.

h. Incident Reporting. Describe the agreements made regarding the reporting of and response to information security incidents for both organizations.

i. Audit Trail Responsibilities. Where applicable, describe how the audit trail responsibility will be shared by the organizations and what events each organization will log. Specify the length of time that the logs shall be retained. If no audit trail is performed, so state.

j. Timeline. Identify the expiration date of the memorandum and procedures for authorizing this.

k. Authority to Disconnect**.** The memorandum may be terminated with written notice from any affected DAA. Responsibilities related to disconnection and reconnection must be described.

l. Consent to Monitor. Approving authorities for networks that connect to an NNSA network must agree to monitor user activity to ensure official use only of NNSA information systems.

m. Consent to Test. Approving authorities for networks that connect to an NNSA network must agree to completion of a remote compliance assessment directed by the NNSA Cyber Security Program Office and/or the NNSA "Red Team" for "site to enterprise" connections and random remote compliance assessment of "site to site" and "site to non-NNSA." The NNSA Cyber Security Program Office will provide prior notification.

n. Account Management. Responsibilities and processes for establishing cross-domain accounts must be documented.

o. Controlled Interface. A control interface is used to control information flow based on the information type; to maintain the confidentiality, integrity, and availability of information being transmitted; and to provide protection services

for the interconnected systems. Refer to DOE Cyber Security Technical and Management Requirements for Interconnected Systems Management (TMR-5) for functional requirements of a controlled interface. A controlled interface must be used in the following circumstances.

(1) For unclassified information systems with different security impact levels, a controlled interface must be used to adjudicate the differences in security policies and practices. Note that in cases where the security impact levels are equal, each system's implemented security controls can be relied on to preserve information confidentiality and Need-to-Know.

(2) For classified information systems with different protection indices, a controlled interface is required to adjudicate the differences in security policies and practices. Note that in cases where the protection indices are equal, each system's implemented security controls can be relied on to preserve information confidentiality and Need-to-Know. However, users are responsible for ensuring that the recipient of information has a Need-to-Know to include formal access to any Sigma level for the information.

(3) A controlled interface must be used when interconnecting NNSA information systems to other systems outside of DOE, such as the Internet, public switch networks, or DOD systems.

p. Review System and Network Accreditations. The introduction of inter-site network connections, including those that affect only one DAA, requires a review of the vulnerabilities and residual risks to the affected NNSA networks and an update to the ISSP. For interconnections that only affect one DAA, all security documentation requirements must be included in the applicable ISSPs for each interconnecting information system.

4. INTER-SITE NETWORK INTERCONNECTION APPROVAL PROCESS. Federal policy requires Federal agencies to establish interconnection agreements. Specifically, OMB Circular A-130, Appendix III, requires agencies to obtain written management authorization before connecting their information technology systems to other systems, based on an acceptable level of risk. The written authorization should define the rules of behavior and security controls that must be maintained for the system interconnection and it should be included in the organization's system security plan. Because the interconnection may affect the security posture for each involved network and/or system, the process for instituting and maintaining the interconnection is intertwined with the process for maintaining an accreditation for each of the networks individually. The process outlined below defines the general steps necessary to initiate and maintain the interconnectivity. Figure XX-1 illustrates the process flow for approval.

a. Define and Review Business Case. A business case must be developed that describes the mission or organizational need for the interconnection. The two affected organizations should work together to assure that the purpose and intent

of the interconnection is of mutual benefit and is aligned with their respective mission requirements, After the interconnection has been established, the business case should be reviewed periodically to confirm that the requirements are still valid.

b. Verify and Review Existing Systems. NNSA information systems being considered for interconnection must be covered by an existing ISSP and an ATO or IATO. Before interconnection can be formally approved, the ISSP and ATO or IATO must be reviewed to verify completion and the inclusion of necessary controls. If the system being considered for interconnection is in the development phase, the draft ISSP must include or reference the interconnection specifics.

c. Develop Formal ISA. The ISA is a security document that specifies the technical and security requirements for establishing, operating, and maintaining the interconnection. It also supports the MOU between the organizations. The ISA documents the requirements for connecting the IT systems, describes the security controls that will be used to protect the systems and data, contains a topological drawing of the interconnection, and provides a signature line. Appendix I is a sample MOU.

d. Develop Formal MOU. The MOU details the management agreement and describes the responsibilities between organizations with interconnected information systems. It documents the terms and conditions for sharing data and information resources in a secure manner. Appendix J is a sample ISA.

e. Revisit of ATO or IATO for Systems. The establishment of a network interconnection may introduce new vulnerabilities and alter the security posture for systems. Both organizations should update their ISSP and related documents to reflect the changed security environment in which their respective system operates.

f. Approve or Reject. The interconnection is approved when both the ISA and MOU have been signed. A formal letter of rejection should be provided by the DAA, if the connection is denied, to indicate the reasons and any additional expectations.

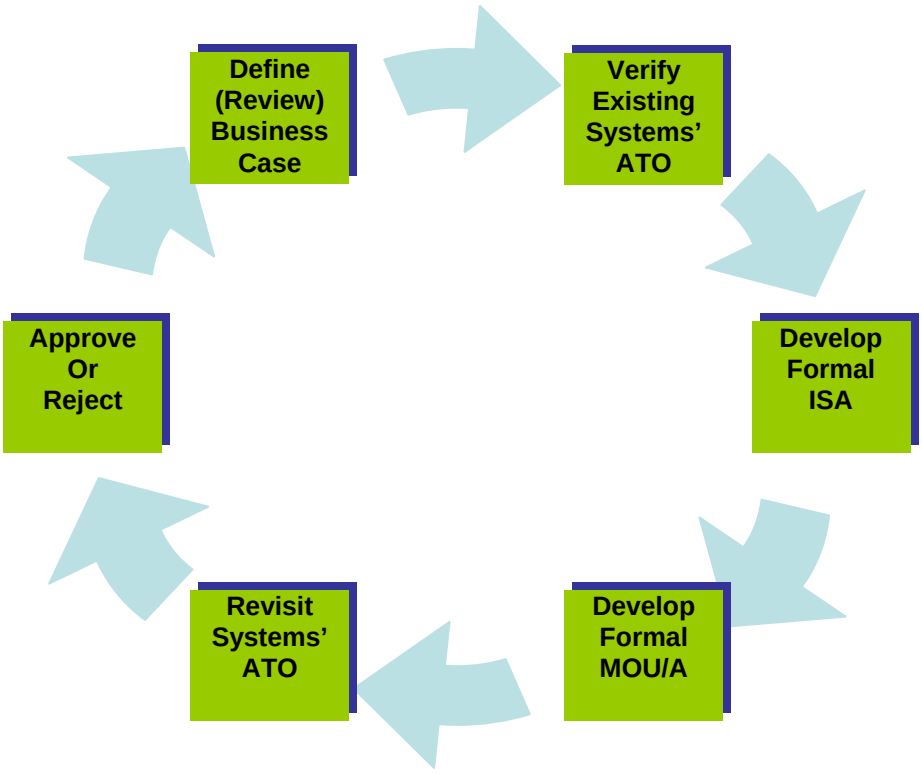


Figure XX-1. Interconnectivity Process Flow

This page intentionally left blank.

APPENDIX A: ACRONYMS

AA	Approving Authority
ATO	Approval to Operate
C&A	Certification and Accreditation
CFO	Chief Financial Officer
CMPC	Classified Matter Protection and Control
CAN	Computer Network Attack
CNE	Computer Network Exploit
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNNSP	Committee on National Security Systems Policy
COMSEC	Communication Security
CSPM	Cyber Security Program Manager
CSPP	Cyber Security Program Plan
DAA	Designated Approving Authority
DCID	Director of Central Intelligence Directive
DOD	Department of Defense
DOE	Department of Energy
ECI	Export Controlled Information
FOIA	Freedom of Information Act
HQ	Headquarters
IATO	Interim Approval to Operate
IATT	Interim Approval to Test
IG	Inspector General
INFOCON	Information Condition
INFOSEC	Information Security
IRM	Information Resources Management
ISO	Information System Owner
ISOM	Information System Security Office Manager
ISSM	Information System Security Site Manager
ISSO	Information System Security Officer
ISSP	Information System Security Plan
IT	Information Technology
LAN	Local Area Network
NAP	NNSA Policy
MC&A	Material Control and Accountability
NIACAP	National Information Assurance Certification and Accreditation Process
NIST	National Institute of Standards and Technology
NISPOM	National Industrial Security Program Operating Manual
NNPI	Naval Nuclear Propulsion Information
NNSA	National Nuclear Security Administration
OMB	Office of Management and Budget
OPSEC	Operations Security
PCSP	Program Cyber Security Plan

PDA	Personal Digital Assistant
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
PTS	Protected Transmission System
SCI	Sensitive Compartmented Information
SP	Special Publication
SSSP	Site Safeguards & Security Plan
TSCM	Technical Surveillance Countermeasures
TEMPEST	not an acronym
UCNI	Unclassified Controlled Nuclear Information
WAN	Wide Area Network

APPENDIX B: GLOSSARY

The following are terms and definitions used in this NAP that are not found in The Committee on National Security Systems (CNSSI) 4009, National Information Assurance Glossary, dated May 2003; revised June 2006. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

Architecture	The configuration of any equipment or interconnected systems or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment and services, including support services and related resources.
Certification and Accreditation (C&A) perimeter (See Perimeter below)	All components of a system that are to be accredited by the DAA and excluding separately accredited systems to which the system is connected.
Configuration Management Plan (CMP)	The CMP describes the methodology and procedures used for controlling configuration changes to information systems that impact the approved security posture. This plan is maintained throughout the C&A process and system lifecycle.
Consequence of Loss	An expression of the consequences of loss of the information's integrity, availability, or confidentiality.
Contingency Plan	Measures established to assist an organization in their ability to quickly and cost effectively restore an information system following a disruption.
Cyber Security	Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.
Cyber Security Incident	A cyber security incident is any adverse event caused by an outsider or an insider that threatens the security of information resources. Adverse events may include compromises of integrity, denial-of-service attacks, compromises of confidentiality, loss of accountability, or damage to any part of

	the system. Examples include the insertion of malicious code, such as viruses, Trojan horses, or back doors, unauthorized scans or probes, successful and unsuccessful intrusions, and insider attacks.
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/Custodian	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.
DAA Representative (DAA Rep)	A technical and programmatic expert in cyber security that performs programmatic and technical reviews and makes operational and approval recommendations for risk acceptance to the DAA. Within the NNSA, the DAA Representative can accept risk.
Destroying	Actions taken to ensure that media cannot be reused as originally intended and information is virtually impossible or prohibitively expensive to recover.
Direct User	A user with physical or electronic access to any component of the information system.
Enterprise Information System	An information system with components within the perimeter that is located on separate facilities or sites.
Foreign National	A person who was born outside the jurisdiction of the U.S. is a citizen of a foreign government, and has not been naturalized under U.S. law.
General Support System (GSS)	An interconnected set of information resources under the same direct management control that share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a Local Area Network (LAN), including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a Departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. [From Office of Management and Budget (OMB) Circular A-130, Appendix III.]

IARC	NNSA Information Assurance Response Center located in Las Vegas, NV. 702-942-2611
Information Integrity	The preservation of unaltered states as information is transferred through the system and between components.
Information System	An information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. The process of uniquely assigning information resources to an information system defines the security accreditation boundary for that system. NNSA elements have flexibility in determining what constitutes an information system *(i.e., major application or general support system)* and the resulting security accreditation boundary that is associated with that information system. Both major applications and general support systems will be treated as an information system (i.e., "system") and will undergo the certification and accreditation process described in NAP 14.2-C.
Information System Security Plan (ISSP)	A formal agreement among the DAA, the ISSM(s), and the system owner(s). It is used throughout the NNSA C&A process to guide actions, and to document decisions, security requirements, certification tailoring and level-of-effort, certification results, ISSM's certification, and the DAA's accreditation to operate.
Information Technology (IT)	The hardware, firmware, and software used as part of the information system to perform information functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. For purposes of the preceding sentence, equipment is used by an executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency, which (1) requires the use of such equipment, or (2)

	requires the use, to significant extent of such equipment, in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services, including support services, and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "information technology" does not include National Security systems as defined in the Clinger-Cohen Act of 1996 (40 U.S.C. 1452). [Office of Management and Budget, Circular A-130, Nov 30, 2000.
Interconnection	The direct connection of two or more information systems for the purpose of sharing data and other information resources. A system interconnection has three basic components: two information systems and the communication mechanism by which data is made available, exchanged, or passed one-way only. Each information system maintains its own intra-system services and controls and protects its own resources.
Key Resources	Publicly or privately controlled resources essential to the minimal operations of the economy and government.
Legacy information system	An operational information system that existed prior to the implementation of the NNSA C&A process.
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]
Mission	The assigned duties to be performed by an information system or site.
Multi-User System	A system, that under normal operations has more than one user accessing it simultaneously. Systems accessed by more than one user sequentially (one user at a time) without undergoing the necessary procedure to remove residual data between users are also considered multi-user systems.
NNSA-Controlled Environment	An area within NNSA-controlled premises or within NNSA

contractor-controlled premises.

NNSA Elements — NNSA HQ Site Organizations, Service Center, Site Offices, NNSA contractors, and subcontractors which may be referred to as NNSA Elements or sites.

Non-Removable Media — Fixed storage devices, such as hard drives, which provide internal information/data storage.

One-way Receive Only Device — Device with a wireless receiver and no transmitter. The device is not capable of transmitting any Wireless RF (i.e., there is no wireless communication between the device and any base station, not even station keeping or "keep alive" signals.)

Personal Computer — A computer built around a microprocessor for use by an individual, as in an office or at home or school, without the need to be connected to a larger computer.

Personally Owned — An item that is owned by an individual and is intended solely for their personal use.

Personally Identifiable Information (PII)

Personal information that is associated to an individual such as social security number; place of birth; date of birth; mother's maiden name; biometric records, fingerprint, Iris scan, DNA; medical history, previous diseases, metric information, weight, height, BP; criminal history; employment history, ratings, disciplinary actions; financial information, credit card numbers, bank account numbers; and security clearance history.

WHAT PII IS:

1. Social Security Numbers in any form are PII
2. Place of Birth associated with an individual
3. Date of Birth associated with an individual
4. Mother's maiden name associated with an individual
5. Biometric record associated with an individual
    a. Fingerprint
    b. Iris scan
    c. DNA
6. Medical history information associated with an individual
    a. Previous diseases
    b. Metric information

c. Weight
d. Height
e. BP

7. Criminal history associated with an individual
8. Employment history associated with an individual
    a. Ratings
    b. Disciplinary actions
9. Financial information associated with an individual
    a. Credit card numbers
    b. Bank account numbers
10. Security clearance history or related information

WHAT PII IS NOT:

1. Phone numbers (Work, home, cell)
2. Street addresses (Home, work, other)
3. E-mail addresses (Work or personal)
4. Digital pictures
5. Birthday cards
6. Birthday e-mails
7. Grade and Step information for Federal Employees
8. Medical Information pertaining to work status (X is out sick today)
9. Medical information included in a health or safety report (X broke their arm when…)
10. Resumes unless it includes SSN
11. Job titles for employment history, resume, or written biography
12. Federal salaries
13. Federal bonuses
14. Written biographies, such as the ones used in pamphlets of speakers.
15. Alma Mater or degree level in biographies
16. Personal information stored by individuals on their personal workstation or laptop (unless a SSN)

Portable Computing Device — Portable Computing Devices are any portable devices that provide the capability to collect, create, process, transmit, store, and disseminate information. They include, but are not limited to, Personal Digital Assistants (PDAs), palm tops, hand-held or portable computers and workstations, non-Web-enabled cell phones, Web based enhanced cell phones, two-way pagers, and wireless e-mail devices.

Privacy Impact Assessment (PIA)

	A PIA is an analysis of how information is handled: (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Pseudorandom Number	Of, relating to, or being a consistent, characteristic form of random numbers generated by a definite, nonrandom computational process.
Removable Media	Nonvolatile electronic storage media that can be physically removed from an information system, meaning the storage media is not attached to the information system via the internal bus. Examples of removable media include diskettes, hard drives, zip drives, thumb drives, tapes, cartridges, optical disks, disk packs, etc.
Reusable Password	A data item associated with a user identifier that remains constant and is used for multiple access requests over some explicit time interval.
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
Security Documentation	All documents which describe the security requirements, design descriptions of security-relevant software and hardware, certification packages, and ISSPs. The ISSP is the basic system protection document and evidence that the proposed system or major application, or update to either, meets the protection requirements.
Security Process	The series of activities that monitor, evaluate, test, certify, accredit, and maintain the system accreditation throughout the system lifecycle.
Security Significant Change	A security significant change is defined as a change that impacts the risk or security posture accepted by the DAA. A security significant change may result from a single change or an accumulation of changes. The change could be an introduction of new technologies, changes in system

	configuration, changes in the systems environment (network, physical, operational), operational procedures, or the identification of vulnerabilities For example, incorporating wireless devices or networks into a wired legacy information system, or identifying new vulnerabilities or threats.
Sensitive Unclassified Information (SUI)	
	SUI includes unclassified information requiring protection mandated by policy or laws, such as Privacy Act information, Official Use Only (OUO) information, Export Controlled Information (ECI), Unclassified Controlled Nuclear Information (UCNI), and Personally Identifiable Information (PII).
Site	An NNSA facility: can be a NNSA Service Center, NNSA Site Office, NNSA contractor or subcontractor facility, or the NNSA HQ Site activity that has a responsibility to protect NNSA information systems. It has a set of geographical boundaries as defined in a NNSA Site Safeguards and Security Plan or Site Security Plan. NNSA sites are also referred to NNSA Element.
Site Manager	The person responsible for management of all activities at a site.
Site Safeguards & Security Plan	The SSSP is a risk management document that describes the Safeguards and Security Program and its vulnerability and risk analyses. SSSP authors draw conclusions in the document that are intended to initiate and guide long-term planning for S&S operations.
Special Character	Any non-alphanumeric character.
System	The set of interrelated components within the same accreditation boundary consisting of mission, environment, and architecture as a whole. A system normally includes hardware, software, information, data, applications, and communications.
System Development Life Cycle (SDLC)	
	A structured approach for systems development from planning and support to disposal of the system.
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.

Trusted Operating System (OS)	An operating system configured to an approved standard.
Weapon Data	Restricted Data or Formerly Restricted Data concerning the design, manufacture, or utilization (including theory, development, storage, characteristics, performance, and effects) of nuclear weapons or nuclear weapon components, including information related to improvised nuclear devices.

This page left intentionally blank.

APPENDIX C: CONTRACTORS REQUIREMENTS DOCUMENT

This appendix provides the Contractors Requirements Document (CRD) for the NNSA CSP.

1. INTRODUCTION. This CRD 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.

2. OVERVIEW. All information collected, created, processed, transmitted, stored, or disseminated by, or on behalf of, the NNSA on automated information systems requires some level of protection. The loss or compromise of information entrusted to NNSA contractors may affect the Nation's economic competitive position, the environment, the National security, NNSA missions, or the citizens of the United States. The risk management approach defined in the NNSA CSP provides for the graded, cost-effective protection of automated information systems containing unclassified or classified information.

   The contractor must systematically integrate cyber security 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 protecting information on information systems for the purpose of maintaining National security and ensuring the continuity of NNSA operations.

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

4. IMPLEMENTATION. A plan for the implementation of this CRD must be completed within 60 days after incorporation of this CRD into the contract. This implementation plan shall not exceed three years from the date of formal approval. Meaning, the NNSA Element's CSP must comply with all requirements set forth in this NAP. Further, all information systems must be protected in accordance with the requirements set forth in this NAP. The implementation plan must include, at a minimum, the program activity to be modified/created; the starting date of revision/ development; the estimated due date; and the responsible party for the stated activity.

5. REQUIREMENTS. Risk-based approaches and other means must be used to evaluate and verify the effectiveness of cyber security measures, to identify areas requiring improvement, and to validate implemented improvements.

   a. Protection Measures. Protection measures for all NNSA information systems must conform to the protection measures described in the NNSA PCSP, CRDs, an

NNSA-approved minimum information system security configuration, the contractor's CSPP, and the ISSP.

b. Information Protection. As a minimum, the protection afforded information, and the information system(s) on which it resides, is based on a risk-based graded protection approach as defined by the NNSA PCSP.

(1) Protection measures may be strengthened based on an assessment of unique local threat(s) or the local evaluation of CoL.

(2) All Government information and any non-Government information on an NNSA information system must be considered when determining the system's protection measures.

6. Information Types/Groups. An Information Group contains all information that requires similar protection or is similar in content or use. All NNSA information must be identified as part of an NNSA-approved information group. Chapter V contains the definition of NNSA Information Groups. Chapter XVII and Appendix B further details what information is considered to be SUI, including PII.

a. Classified Information Access. Access to classified information must be granted only to persons with the appropriate access authorization and Need-to-Know in the performance of their duties according to NNSA policies and DOE M 470.4-5, *Personnel Security*.

b. Unclassified Information Access. Access to unclassified information must be granted to only those persons who have the appropriate Need-to-Know for the information in the performance of their duties. The individual disseminating the information is responsible for determining the recipient's Need-to-Know in accordance with the site's processes and NNSA policies and guidance.

c. Knowledge and Resources. All contractor personnel must possess the knowledge, skills, equipment, and resources to fulfill their cyber security responsibilities under both normal and emergency conditions.

d. Facility Clearance and Registration. Contractors with classified information systems must obtain prior approval through the Facility Clearance and Registration Process as outlined in DOE M 470.4-1.

e. Risk Management Process. The contractor must implement the risk management processes described in Appendix H.

f. Configuration Management. The contractor must implement NNSA CM policies for all information systems managed by the contractor as described in Chapter III.

g. Cyber Security Program Plan. The contractor must implement the CSPP processes described in Chapter IV.

h. Deviations. The contractor must implement the deviation process as described in Chapter VI.

i. Incident Management. Contractors must implement the criteria and processes for cyber security incident preparation, prevention, warning, reporting, and recovery involving NNSA information systems as defined in Chapter VII.

j. INFOCON. Contractors shall develop and implement standardized procedures and responsibilities for authorizing and communicating INFOCONs throughout the NNSA as described in Chapter VIII.

k. Plan of Actions and Milestones (POA&M). Contractors must establish a POA&M process for tracking and mitigating CSP and system-level weaknesses as described in Chapter IX.

l. Vulnerability Management. Contractors must implement a vulnerability management program, to include patch management procedures, as described in Chapter X.

m. Portable Computing Devices. Contractors shall implement the criteria and processes for the use of non-Government owned or Government-owned portable computers as defined in Chapter XI.

n. Password Protection. Contractors shall implement policies for the generation, protection, and use of passwords to support authentication when accessing classified and unclassified NNSA information systems, applications, and resources as described in Chapter XII.

o. Wireless, Remote, and Peer-to-Peer (P2P) Technologies. Contractors must implement minimum security controls as described in Chapters XIII, XIV, and XV to appropriately protect NNSA information assets when implementing wireless, remote access, and P2P technologies.

p. Contingency Planning. Contractors must implement contingency planning procedures as described in Chapter XIIII for NNSA information systems for which they are responsible.

q. Foreign National Access. Contractors must define requirements for allowing Foreign National Access to NNSA information systems to include, but not limited to computers, networks, associated servers, data storage devices, and portable/mobile devices as described in Chapter XX.

7. RESPONSIBILITIES.

a. Laboratory Director or Production Facility Manager. The Laboratory Director or Production Facility Manager must:

(1) Assume responsibility and accountability for the contractor's CSP.

(2) Appoint, in writing, an ISSM responsible for implementing the NNSA PCSP at all facilities under the contract.

(3) Ensure the appointment of an ISSO for each information system as described by an ISSP managed or operated by the contractor.

(4) Ensure adequate resources are allocated to the contractor's CSP, including applicable Enterprise Information Systems and Major Applications.

(5) Coordinate on Enterprise System and Major Application CSPPs.

(6) Ensure that the effectiveness of the CSP is monitored through self-assessments and reviews.

(7) Ensure the development, implementation, and maintenance of the contractor ISPP.

(8) Submit the contractor's CSPP to the cognizant Site Office or Service Center for approval.

(9) Ensure the contractor's ISSM, ISSO, ISO, users, and System Administrators are trained in their specific duties and the technologies for which they have responsibilities.

b. Information System Security Site Manager (ISSM). The ISSM is appointed by the Laboratory Director or Production Facility Manager and is responsible for development of the contractor's CSPP and implementation of the CSP. The ISSM must have a working knowledge of system functions, cyber security policies, and cyber security protection measures.

(1) Maintains record copies of the contractor's CSPP and ensures that a record copy of each ISSP is maintained.

(2) Appoints ISSOs for information systems operated by the NNSA Element and ensures that each ISSO and system administrator is aware of and fulfills their cyber security duties as described in the PCSP and the Element's CSPP.

(3) Ensures the development, documentation, and presentation of information systems security education, awareness, and training activities for contractor management, cyber security personnel, application owner, data steward, and users.

(4) Ensures that users are trained on the information systems cyber security features, operation, and safeguards prior to being allowed access to the system.

(5) Ensures that ISSOs and systems administrators are trained on information systems cyber security requirements, operations, safeguards, INFOCON, and incident handling procedures.

(6) Establishes, documents, and monitors the contractor's CSP implementation and ensures contractor compliance with the NNSA PCSP. Upon completion of each assessment or review, the ISSM must ensure that a corrective action plan is prepared and implemented for all findings or vulnerabilities as directed by DOE M 470.4-1.

(7) Identifies and documents, in coordination with the contractor's Operations Security (OPSEC) program, site-specific threats to information systems and information at the site.

(8) Develops and documents additional or modified protection measures for those threats and identifies any site-wide protection measures/practices that apply to all site systems.

(9) Obtains approvals for modified protection measures from the cognizant DAA.

(10) Ensures the CSPP is coordinated with other site plans and programs to include: disaster recovery, Site Safeguards and Security Plan (SSSP) or Site Security Plan, Classified Matter Protection and Control, Physical Security, Personnel Security, Telecommunications Security, TEMPEST, Technical Surveillance Countermeasures, Operations Security, and Nuclear Materials Control and Accountability.

(11) Ensures the development of procedures to implement the contractor's CSP on all information systems.

(12) If appointed as the Certification Agent, certifies to the cognizant DAA that the protection requirements described in the ISSP for each information system have been implemented and are operational.

(13) Ensures that the cognizant DAA is notified when the information system is no longer needed or when changes occur that might affect the accreditation of the information system.

(14) Participates in CSPM sponsored cyber security training within six months of their appointment.

(15) Ensures the development, documentation, and presentation of cyber security training for escorts in information systems operational areas.

(16) Ensures a DAA-approved overwrite method is used for sanitization and a review of the results of overwrites to verify that the method used completely overwrote all classified or sensitive information.

(17) Ensures that each information system user acknowledges, in writing or electronically their responsibility (Code of Conduct) for the security of information systems and information.

(18) Communicates individual incident reports to the ISOM so that the DAA can meet their reporting schedule.

(19) Ensures investigation and documentation of suspected cyber security incidents, categorization of incidents as Type 1, Type 2, or No Incident, and retention of documentation.

(20) Ensures analyses of and corrective actions for incidents and findings with status reporting to the DAA.

(21) Conducts self-assessments in accordance with NNSA requirements.

(22) Ensures each individual responsible for major applications within the site is aware of and fulfills their cyber security duties as described in the NNSA PCSP and the contractor's CSPP.

(23) Recommends changes in the NNSA site INFOCON status to the DAA.

c. Information System Owner. The ISO is the person or organization that is responsible for acquiring, operating or upgrading an information system. The ISO coordinates all aspects of the system for which he or she is responsible from initial concept, through development, to implementation and system maintenance. The information system owner:

(1) Ensures the preparation of the ISSP and the certification and accreditation package.

(2) Ensures the certification and accreditation of all information systems under their cognizance.

d. Information System Security Officer (ISSO). The following roles and responsibilities apply to all information system for which the ISSO is responsible. Multiple information systems may be assigned to a single ISSO. ISSOs are responsible to the ISSM for fulfilling their duties.

(1) Ensures the implementation of protection measures that are documented in the ISSP for each information system for which they are the ISSO.

(2) Ensures that privileged users are granted access to information system's resources based on the least privilege principle.

(3) Identifies, in coordination with the ISSM, and documents in the ISSP, unique threats to information systems for which they are responsible.

(4) Ensures that the CoL of confidentiality, integrity, and availability for the information is determined prior to use of an information system.

(5) Documents any special protection requirements identified by the application owner, data owner, or data steward and ensure that these requirements are included within the protection measures implemented in the information system.

(6) Ensures each information system for which they are the ISSO is covered by an ISSP.

(7) Maintains a recorded copy of the ISSP for each information system for which they are the ISSO.

(8) Ensures the implementation of site procedures defined in the site CSPP and the ISSP for each information system for which they are the ISSO.

(9) Ensures that the cognizant ISSM is notified when an information system is no longer needed or when changes occur that might affect the accreditation of the information system.

(10) Ensures that information access controls and cyber protection measures are implemented for each information system as described by its ISSP.

(11) Ensures that users and systems administrators are properly trained in information system security by identifying cyber security training needs and the personnel who need to attend the cyber security training program.

(12) Conducts cyber security reviews and tests to ensure that the cyber security features and controls are functioning and effective.

(13) Participates in the ISSM's self-assessment and training programs.

(14) Ensures a risk assessment has been conducted for the system for which they are responsible.

(15) Communicates individual incident reports to the ISSM to allow for the ISSM to meet their reporting schedule.

(16) Ensures the implementation of all applicable protection measures for each information system for which they are responsible.

(17) Ensures that unauthorized personnel are not granted use of, or access to, the information system.

e. Application Owners/ Data Owners/Data Stewards. These roles and responsibilities apply to all information systems.

(1) Determine and declare the sensitivity of the information prior to its being created, processed, stored, transferred, or accessed on the information system.

(2) Identify unique threats to their information and ensure that that such information is provided to the ISSO and ISSM.

(3) Advise the ISSO of any special confidentiality, integrity, or availability protection requirements for the information.

(4) Ensure that the information is processed only on a system that is approved at a level appropriate to protect the information.

(5) Determine and document the data and application(s) that are essential to fulfill the organizational mission to identify the criticality of the system and ensure that requirements for contingencies are determined, implemented, and tested.

(6) Approve access to their information.

(7) Ensure applications and/or data supporting Critical Infrastructure or Key Resources are identified.

(8) Provide resources to support the implementation and testing of CPs for the application data.

f. Users. The roles and responsibilities apply to all cyber assets.

(1) Comply with the requirements of the NNSA PCSP, the contractor's CSPP, and the information system ISSP.

(2) Be aware of, and knowledgeable about, their responsibilities in regard to information systems security.

(3) Ensure that any authentication mechanisms, including passwords, issued for the control of their access to information on information systems are not shared and are protected at the same level of protection applied to the

information to which they permit access, and report any compromise or suspected compromise of an authenticator to the appropriate ISSO.

(4) Be responsible and accountable for their actions on an information system.

(5) Acknowledge via electronic signature or in writing their responsibilities (Code of Conduct) for protecting information systems and classified information.

(6) Participate in training on the information system's prescribed security restrictions and safeguards before initial access to a system. As a follow-up to this initial training, participate in an ongoing security education, training, and awareness program.

(7) Immediately report all security incidents and potential threats and vulnerabilities involving the information system to the appropriate ISSO.

(8) Ensure that system media and system output are properly classified, marked, controlled, and stored.

(9) Protect terminals from unauthorized access as described in the information system ISSP.

(10) Inform the ISSO when access to a particular information system is no longer required, such as at the completion of a project, or a transfer, retirement, or resignation.

(11) Observe rules and regulations governing the secure operation and authorized use of information systems.

(12) Use the information system only for official Government business or other activities authorized by NNSA, the Laboratory Director, or Production Facility Manager.

g. Privileged Users.

(1) The number of privileged users must be limited to the minimum number needed to manage the system.

(2) All privileged users must be responsible for all requirements for general users.

(3) Privileged users are responsible to ensure that user access to the information system’s resources and information is based on the least privilege principle.

(4) All privileged users must:

(a) Be U.S. citizens, unless otherwise approved in accordance with the approved contractor CSPP or in writing by the cognizant DAA.

(b) Possess approvals of Need-to-Know for all information on the system.

(c) Possess an Access Authorization sufficient for access to the highest classification and most restrictive category of data processed on the information system.

(d) Use unique identifiers as described in the information system ISSP.

(e) Protect the root or super-user authenticator at the highest level of data it secures.

(f) Be responsible for all super-user or root actions under their account.

(g) Report any and all security relevant information system problems to the ISSO.

(h) Use the special access or privileges granted only to perform authorized tasks and functions.

h. Certification Agent . The Certification Agent (CA) is designated to perform security certification where certification is the comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. The ISSM may fulfill the role of the CA. General duties of the certifier include:

(1) Ensuring that risk analyses and security evaluations are completed prior to information system, network and application certification.

(2) Certifying the extent to which systems, networks and applications meet prescribed security requirements.

(3) Preparing the certification report and forwarding the report after certification is completed to the ISSM with any recommendations on accreditation. If the ISSM is the CA, then the report will be forwarded to the DAA.

(4) Maintaining and providing other records and reports of certification activities, as necessary.

(5) Reviewing all information contained in the ISSP.

(6) Evaluating the technical and non-technical security features of an information system and other safeguards made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

This page intentionally left blank.

APPENDIX D: RECOMMENDED ACTIONS FOR INFOCON LEVELS

Table D-1. Recommended Actions for INFOCON Levels

LABEL (DESCRIPTION)	CRITERIA	RECOMMENDED ACTIONS
GREEN	No significant activity. Normal operations. General threat unpredictable.	Ensure all mission critical information and information systems (including applications and databases) are identified. Ensure all points of access and operational necessity are identified. On a continuing basis, conduct normal cyber security practices. Periodically review and test higher INFOCON actions.
BLUE	Indications and warnings (I&W) indicate general threat. Regional events occurring that affect US interests and involve potential adversaries with suspected or known CNA capability. Information system probes; scans or other activities detected indicating a pattern of surveillance. Increased and/or more predictable threat events Nation- or Internet-wide computer network exploit. Incident occurs at NNSA or DOE site. Intelligence indicates imminent attack against NNSA or DOE,	Accomplish all actions at INFOCON Normal, plus the following: Execute appropriate cyber security practices. Heighten user awareness. Execute appropriate defensive actions. Follow NNSA reporting procedures identified in NNSA cyber security policies. Review higher INFOCON actions. Consider proactive execution of some, or all, higher INFOCON actions.

LABEL (DESCRIPTION)	CRITERIA	RECOMMENDED ACTIONS
YELLOW	I&W indicate targeting of specific system, location, unit or operation. Significant level of network probes, scans or activities detected indicating a pattern of concentrated reconnaissance. Network penetration or denial of service attempted with no impact to NNSA or DOE operations. Incident occurs at NNSA site that affects an NNSA enterprise system or may impact another NNSA site. Intelligence indicates imminent attack against NNSA or DOE site.	Accomplish all actions at INFOCON BLUE, plus the following: Execute, as appropriate, the following cyber security practices (recommended practices in NNSA cyber security policies) Increase level of auditing on critical systems. Immediately review for security, and patch, as needed, all critical systems. Consider limiting connections and traffic that cross site perimeter. Isolate compromised systems immediately. Follow NNSA reporting procedures identified in NNSA cyber security policies. Review higher INFOCON actions. Consider proactive execution of some, or all higher INFOCON actions.
ORANGE	Intelligence attack assessment(s) indicate a limited attack. Information system attack(s) detected with limited impact to NNSA or DOE operations: • Minimal attack success, successfully counteracted. • Few or no data or systems compromised. • Site able to accomplish mission. • Computer Network Exploit at a DOE or NNSA site. • Nation- or Internet-wide computer network exploit. • Intelligence indicates imminent attack against national infrastructure or National Security element.	Accomplish all actions at INFOCON YELLOW, plus the following: Execute, as appropriate, the following cyber security practices (recommended practices in NNSA cyber security policies) Increase level of auditing on critical systems. Minimize connections and traffic to absolute minimum needed for current mission operations. Reconfigure systems to minimize access points and increase security. Consider disconnecting all non-mission-critical systems and networks from the Internet. Isolate any compromised systems immediately. Follow NNSA reporting procedures identified in NNSA cyber security policies. Review higher INFOCON actions. Consider proactive execution of some, or all, higher INFOCON actions.

LABEL (DESCRIPTION)	CRITERIA	RECOMMENDED ACTIONS
RED	Successful information system attack(s) detected which impact NNSA operations. Widespread incidents that undermine ability to function effectively. Significant risk of mission failure. Computer Network Attack against national infrastructure or National Security element.	Accomplish all actions at INFOCON ORANGE, plus the following: Execute, as appropriate, the following cyber security practices (recommended practices in NNSA cyber security policies). Designate and reconfigure information systems and networks to use controlled connections and traffic. Execute procedures for ensuring graceful degradation of information systems and network(s). Disconnect all non-mission-critical systems and networks from Internet. Implement procedure for 'stand-alone" or manual operations. Follow NNSA reporting procedures identified in NNSA cyber security policies. Execute applicable portions of Continuity of Operations plans.

This page left intentionally blank.

APPENDIX E: FACTORS INFLUENCING INFOCON

When determining the appropriate defensive posture, many factors must be considered. This appendix lists several factors that managers should consider when determining the INFOCON. Note that this list is offered as broad guidance; other factors may also be considered.

- Other indications and warnings (including domestic threats). NSA IPC Alerts; National Infrastructure Protection Center (NIPC) advisories, threats, warnings; and law enforcement agency intrusion reports.
- CNA intelligence assessments.
- Current world situation. Increased tensions with a nation possessing CNA capability may precede CNA operations against us.
- Other alert systems such as SECON, etc. Managers must determine if a change in one alert status will cause a corresponding change in another alert status.
- Dependence of NNSA functions upon particular information systems. This type of analysis may suggest the degree to which a particular network, system, application or database is mission critical.
- Manager's assessment of mission-critical information system readiness. This readiness may be determined from the networks' security posture, vulnerability, extent of compromise, etc.
- Manager's assessment of readiness to coordinate the protection of critical infrastructure and key resources identified under Homeland Security Presidential Directive-7 (HSPD-7), *Critical Infrastructure Identification, Prioritization, and Protection*
- Incident reports. These are roughly analogous to attack assessment.
- Trend analyses. Reports showing number, type, and frequency of attacks, systems targeted, and hot IP addresses.
- Technical impact assessment. This information may be included in an incident report or may result from follow-on analysis. This assessment may include the extent of system compromise and/or disruption and the degree to which system confidentiality, integrity, availability, and authentication have been affected.
- Operational impact assessment. A key element in determining the INFOCON. See Appendix F. The process for assessing operational impact also lays the groundwork for executing preventive measures, developing workarounds, and establishing restoration priorities.
- ISSM's assessment of the potential for an information attack. Although much objective data is available on which to base the decision, the final judgment for declaring an INFOCON change rests with the DAA. Objective assessment of the situation and prudent analysis of all available information must be integrated with the manager's experience and leadership to determine the organization's appropriate defensive posture.

This page intentionally left blank.

APPENDIX F: OPERATIONAL IMPACT ASSESSMENT

Assessing the impact of CNE and CNA on our ability to conduct operations is key to conducting damage assessment, prioritizing response actions, and assisting in identifying possible adversaries. This appendix offers an operational impact assessment process that may be used when reporting changes in INFOCON. Note that assessment results are classified SECRET at a minimum. The assessment process itself is unclassified.

Prior to an attack:

- Identify all critical information systems.
- For each critical information system, identify all resident critical applications and databases.
- Determine which NNSA functions are supported by each application or database

After an attack or attempted attack has been detected:

- Identify all critical information systems that are, or appear to be, targeted.
- For each information system targeted, determine the technical impact, such as to what degree are confidentiality, integrity, availability, and authentication affected? What critical applications and databases are impacted?
- For the technical impacts identified, estimate the time and resources required to restore functionality. Identify any interim workarounds.
- Determine how the technical impact of the attack affect the organization's ability to function.
- Determine how the impact to the organization's ability to function affect support to current/projected operations? If no specific operations are ongoing or projected, determine how is general capability or readiness affected?

This page intentionally left blank.

APPENDIX G: CONTINGENCY PLAN STRUCTURE

Table G-1. Contingency Plan Structure

Plan Content	Critical Infrastructure Systems	Key System Resources	Remaining Systems
Introduction			
Purpose	X		
Applicability	X		
Scope	X	X	X
References/Requirements	X		
Record of Changes	X		
Concept of Operations			
System Description	X	X	X
Line of Succession	X	X	X
Responsibilities	X	X	
Notification/Activation			
Notification Procedures	X	X	X
Damage Assessment	X	X	
Plan Activation	X	X	X
Recovery			
Recovery Sequence	X		
Recovery Procedures	X	X	X
Facility Access	X	X	
Internal/External Notification	X	X	
Administrative Support	X	X	
Hardware Installation	X	X	X
Media Backup	X	X	X
Software Restoration	X	X	X
Data Restoration	X	X	
Functional and Security Testing	X	X	X
User Notification	X	X	X
Operating Environment	X	X	X

Plan Content	Critical Infrastructure Systems	Key System Resources	Remaining Systems
Reconstitution			
Infrastructure Support	X	X	X
Hardware/Software Installation	X	X	
Internal and External Networking	X	X	X
Functional and Security Testing	X	X	X
Data Restoration	X	X	
Contingency Shutdown	X	X	
Contingency Termination	X	X	
Securing Contingency Site	X	X	
Personnel Return	X	X	

APPENDIX H: RISK ASSESSMENT METHODOLOGY

NNSA Risk Assessment Methodology (RAM) Guidelines

DRAFT Version 1.0

September 13, 2007

Table of Contents

Appendices

Figures

Tables

ACKNOWLEDGEMENT

The Risk Assessment Methodology within NNSA Policy (NAP) 14.1-C was developed by a NNSA Cyber Security Work Group comprised of both Federal and contractor staff and was reviewed by the Designated Approval Authority Council comprised of all Federal staff. The Work Group was chaired by Kimberly Rasar (Deputy Associate CIO for Cyber Security) and members were Miguel Adams, Ernie Crossland, Gus Dahik, Michael Denton, Mark Schaffer, Rex Stratton, and Patricia Valles.

The NAP 14.1-C was developed through a process that was informed by input from the NNSA Management and Operating Contractors. The work group was chaired by Sue Flores (Designated Approval Authority, Service Center) and comprised of the NNSA Designated Approval Authority Council. The NAP 14.1-C is approved through the NNSA Directives Process.

"I would like to thank these individuals for bringing the Risk Assessment Methodology and the NAP 14.1-C to a high quality and successful completion through their hard work, insights, and innovation."

Wayne Jones,
Associate CIO for Cyber Security

CHAPTER I. INTRODUCTION

1. PURPOSE.

The purpose of the Risk Assessment Methodology (RAM) is to provide the NNSA with a repeatable procedure to conduct information technology risk assessments to use during the information system's entire life-cycle. The RAM satisfies one element of the entire risk management process by helping to identify and analyze risk. As one part of the overall risk management process, NNSA and NNSA Elements will use the RAM to understand agency threats and threat sources.

As suggested by A Classification Scheme for Risk Assessment Methods (Campbell, P. & Jason Stamp, 2004), although risk suggestion can be an art form qualitatively surmised, a documented and repeatable process can help raise the information system's level of assurance by increasing the system's performance level, reducing loss, and minimizing risk through building on a framework of risk assessments. Building on a continual risk assessment process will raise an understanding of the threats associated with a system. The results will help satisfy the certification and accreditation (C&A), package risk assessment requirement, IAW NAP 14.2-C, and may be presented as a stand-alone report to the OCIO, CSPM, or local DAA. Furthermore, a repeatable procedure will help satisfy management's continuous monitoring role and due diligence responsibility.

2. OBJECTIVE.

Campbell and Stamp categorize three categories of assessment methods (Campbell 2004):

- The "temporal" method focuses on technological tests used to evaluate the system's performance under stress
- The "comparative" method compares a procedure against a standard
- The "functional" method balances the approaches of the temporal and comparative methods for a balanced risk assessment method.

As part of the information security program of the NNSA, the RAM provides NNSA Elements with a functional framework used to satisfy the risk assessment and help deliver a systematic and repeatable method in producing a risk assessment to the OCIO, CSPM, local DAA, and certification team. The risk assessment method helps to mitigate inherent weaknesses in all of information system products, procedures, and services. In addition, the method will help to provide the NNSA Elements with a historical record of the assumptions reached during the procedure that can increase the risk assessment's level of assurance during subsequent and review periods.

In other words, the process will build on previous knowledge and continually improve through adaptation of historical, current, and future potential risks.

3. REQUIREMENTS.

This process satisfies the requirements set forth in OMB Circular A-130, Appendix III; the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347; and the NAP 14.2-C.

3.1 RAM Frequency

Risk assessments are part of the system's life-cycle. C&A policy requires a risk assessment during the process of certifying and accrediting an information technology system, and when reaccrediting a system on a minimum three year schedule. In addition, the risk assessment can help build on the system's threat statement. At a minimum, a risk assessment must be conducted on the information system:

- During the C&A mandated periods, or at the three-year C&A reaccreditation (see note).
- After an incident on or that affected the information or information system
- A raise in the vulnerability awareness, for example, after system penetration tests.
- DAA directed
- CSPM directed
- OCIO directed.

The RAM is a dynamic and continually evolving process within the overall NNSA cyber security strategic mission.

Note: A re-assessment of the information system's security controls is required on a yearly basis, and the risk assessment includes an assessment of the security controls. Conducting a risk assessment on a yearly basis will fulfill both of these requirements.

3.2 Concept Definitions.

This paragraph defines the concepts described in the RAM Guidelines.

- Risk
- Risk assessment
- Threat
- Threat source
- Vulnerability
- Likelihood
- Likelihood determination
- Impact

Notice that, by the definition's very nature, the unknowns of a risk assessment will contain both objective and subjective elements. The risk assessment mitigates a vulnerability to the information system by providing the functional analysis needed to conduct a risk assessment.

Risk — Risk is a function of the likelihood of a given threat source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.

During the risk assessment process, several independent and unknown factors will determine risks inherent in all systems, process, and procedures. These factors include:

- Likelihood that a threat will occur to the information system
- Likelihood that a threat will result in an adverse impact to the information system
- Severity in an actual attack to the information system
- Threat source of the attack
- Vulnerability of the attack.

Risk Assessment — Risk assessment is the process of characterizing the system; identifying threats and vulnerabilities to the system; determining the likelihood, impact, and risk determination to the system; recommending controls or countermeasures against the vulnerabilities, and documenting the results to fulfill the requirements in 14.2-C, and OMB Circular A-130.

Threat — A threat is the possibility, or probability, that a threat source will exploit a particular vulnerability, or weakness, of a given asset. A threat cannot exploit an asset if there is not weakness. Unfortunately, weaknesses exist in most, if not all of our assets, and careful consideration is required in this analysis, or risk jeopardizing the analysis by overwhelming the security features. An overwhelmed analysis will only confuse the assessment, serving no purpose, however, a careful and concise study of the threat sources entrance (boundary) and motivation will serve the enterprise well.

Threat Source — The threat agent that has the potential of exploiting a vulnerability or weakness in the system. Threat sources can be human events (intentional or unintentional), natural events (for example, hurricane, tornado, flooding), or environmental events (weak building structure, or heating, ventilation, or air conditioning).

Vulnerability — A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (intentional or unintentional) and result in a security breach or a violation of the system's security policy.

Likelihood — The possibility (High, Moderate, or Low) that a threat source will succeed in breaching vulnerability (weakness).

Likelihood Determination — Consideration of the threat sources' motivation and capability of exploiting vulnerability, the nature of the vulnerability, the existence of security controls, and the effectiveness of mitigating security controls.

Impact — The effect of the successful breach in the system and/or information, confidentiality, integrity, availability, or non-repudiation.

4. APPENDICES

There are four appendixes to this document. These include the following:

1. Appendix A lists the acronyms used in this document.
2. Appendix B provides a sample questionnaire form.
3. Appendix C provides sample interview questions.
4. Appendix D lists the references used in this document.

CHAPTER II. RISK ASSESSMENT PROCESS

A risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with a system throughout its System Development Life Cycle (SDLC). The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

To determine the likelihood of a future adverse event, threats to a system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of a vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the assets and resources affected (for example, the criticality and sensitivity of the system components and data). The risk assessment methodology encompasses nine primary steps. These steps are consistent with the Risk Assessment steps described in NIST SP 800-30, Risk Management Guide for Information Technology Systems.

Notice that, in several instances, step names differ; where there is a name difference, the NIST step is displayed in brackets.
Table 1 lists the nine steps are discussed in the sections below:

Table 1. Risk Assessment Steps

Step	Topic
1	System Characterization
2	Threat Analysis [Threat Identification]
3	Vulnerability Identification
4	Analysis of Protection Measures [Controls Analysis]
5	Likelihood Determination
6	Impact Analysis
7	Risk Determination
8	Protection Requirement Recommendations [Control Recommendations]
9	Results Documentation

Steps 2, 3, 4, and 6 can be conducted in parallel after Step 1 has been completed.

2.1 System Characterization.

Step 1 in the RAM process is Build an asset-based threat profile of the system. For the purposes of the RAM, the system is a combination of hardware, software, people, contract vehicles, policies, interfaces, and information. The system may or may not be networked to other information systems, it may be a standalone personal computer, a personal electronic device (PED), or the system may be an enterprise network with server and client relationships. Regardless, the system's function is to processes NNSA information or NNSA-related information that requires protection.

This section describes the system-related information used to characterize a system and its operational environment. Several information-gathering techniques that may solicit information relevant to the system's processing environment are provided. The methodology described in this document can be applied to assessments of single, multiple, or interrelated systems. In the latter case, it is important that the domain of interest and all interfaces and dependencies be well defined prior to applying the methodology.

System-Related Information

Identifying risk for a system requires a keen understanding of its assets. Step 1 in the process describes the collection of system-related information. The step aligns assets to current security practices, begins to identify potential vulnerabilities, and prioritizes critical assets.

The threat profile gathers system information by collecting knowledge of the system. Use the following steps to gather information relating to the system:

1. Step 1.a: Build an asset-based profile
2. Step 1.b: Identify current security practices
3. Step 1.c: Identify current organizational and system vulnerabilities (weaknesses)
4. Step 1.d: Identify and prioritizing critical assets

Step 1a: Build an asset-based profile

A comprehensive protect and defend philosophy requires a full accounting of all the assets within the system. The RAM process is designed to build threat scenarios based on system assets, and this collection of system assets can help satisfy the NNSA C&A risk assessment requirement in 14.2-C.

The asset descriptions below describe typical assets found in a system. The list does not impose additional requirements under the C&A policy, but it used to describe the complexity in defining assets that may pose a risk to the information system.

This list is not comprehensive.

Typical system assets include:

- Likelihood that a threat will occur to the information system
- People—information system users, maintainers, operators, support personnel
- Data and information—classified or unclassified data process by the system
- Automated or manual procedures and/or system support processes - work instructions, manuals, standard operating procedures
- Software—self explanatory
- Hardware—information technology and networking components
- Policies, standards, or procedures—auditing policies/procedures, account creation, hiring practices, or termination procedures
- Information technology standards or protocols—TCP/IP, FTP, SMTP, H.323
- System interfaces—interconnected systems outside of C&A boundary
- Contract support vehicles—memorandums of understanding, service level agreements, and off-site contract support vehicles
- Physical environment—server room, HVAC, doors and alarms, and fire extinguishers
- Logical environment—domains, enclaves, access control methods

Step 1.b: Identify current security practices

Build a list of current security practices against the asset. Note that security practices differ from current security policies. Practices account for how something is done. Policies may direct how something is to be done.

Step 1.c: Identify current organizational and system vulnerabilities (weaknesses)

With knowledge of current security practices, list the potential weakness against current practices, or list what the organization could do better. This step is not a comprehensive security, testing, and evaluation (ST&E). It is a reasonable analysis of the vulnerabilities presented based on the organization's current security practices against the asset. For example, suppose the firewall access control change procedures were unstipulated and allowed unvetted changes to the system. The vulnerability or weakness presented in the change management process could easily open a vulnerable port. ST&E testing is in paragraph 2.3, Vulnerability Identification (Step 3) of the RAM process.

Step 1.d: Identify and prioritize critical assets

Map and prioritize critical assets to determine what the organization's priorities based on asset protection and influence to the information's security requirements. This priority order only helps to identify the organization's critical assets. Table 2 provides a guide to the sample outcome derived from Steps 1.a through 1.d previously described. The priorities are listed in descending order, with 1 being the highest priority.

Table 2. Asset Evaluation Table

Asset Priority	Asset Description	Current Security Practice	Vulnerability Description
4	Servers	Entry control	Tailgating possible
		HVAC	No gauges or lack of accuracy
		Warranty	Expires in one year
2	Software (operating system)	System Administrators	Root access is controlled by one person log on
		Configuration management	Baseline open to modification
		License	None
1	People	Roles and responsibilities	No acknowledgement forms
		FISMA training	Not 100% accountable
		Policy adherence	No metric
		Termination procedures	None
		Incident reporting	Not tested
3	Firewall	Authorized ports and protocols	No change control
		Authorized administrators	Not updated

Note: The information contained in this table is for illustration purposes only.

Information-Gathering Techniques

This topic describes the information gathering techniques used in identifying current security practices. During the identification and building of an asset profile (Steps 1.a through 1.d), the following information-gathering techniques should be employed:

> **Questionnaires.** To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned or used for the system. This questionnaire should be distributed to the applicable technical and nontechnical management personnel who are designing or supporting the system. The questionnaire could also be used during on-site visits and interviews. Appendix B provides sample questionnaire forms used in risk assessments.
>
> **On-site Interviews.** Interviews with system support and management personnel can enable risk assessment personnel to collect useful information about the system (for example, how the system is operated and managed). On-site visits also allow risk assessment personnel to observe and gather information about the physical, environmental, and operational security of the system.

Appendix C contains sample interview questions asked during interviews with site personnel to achieve a better understanding of the operational characteristics of an organization. For systems still in the design phase, the on-site visit would be face-to-face data gathering exercises, and could provide the opportunity to evaluate the physical environment in which the system will operate.

Use of Automated Scanning Tool. Proactive technical methods can be used to collect system information efficiently. For example, a network mapping tool can identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target systems. Information gathering can be conducted throughout the risk assessment process, from Step 1, (System Characterization) through Step 9 (Results Documentation).

2.2 Threat Analysis [Threat Identification]

From the list of identified assets in Step 1, Step 2 identifies potential threats to the assets. This process will help in producing a specific threat statement for the information system. It begins to formalize the critical thinking of threats to individual assets based on threat source, threat introduction or boundary, threat source motivation, effect to security requirement (confidentiality, availability, and integrity), and impact level should the threat occur. Categorizing potential threats to the assets, regardless of probability, will help to analyze all possibilities. Step 5 determines likelihood of the attack.

Figure 1 provides an overview of the entire process in the Threat Identification (Step 2) step.

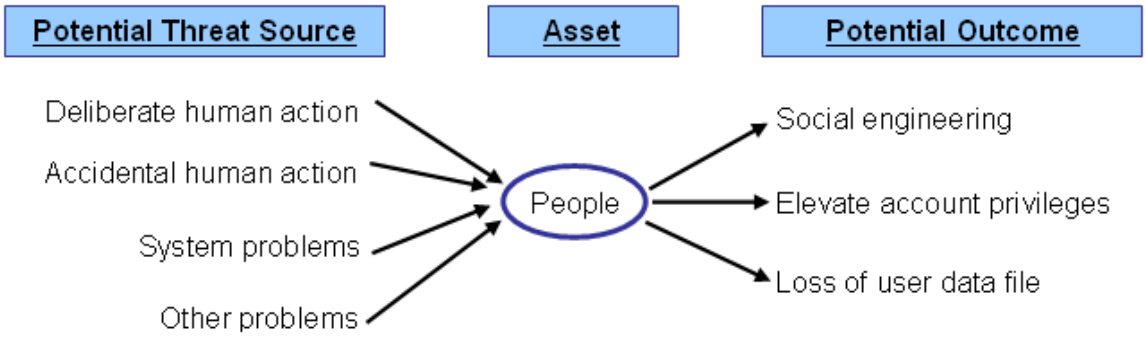
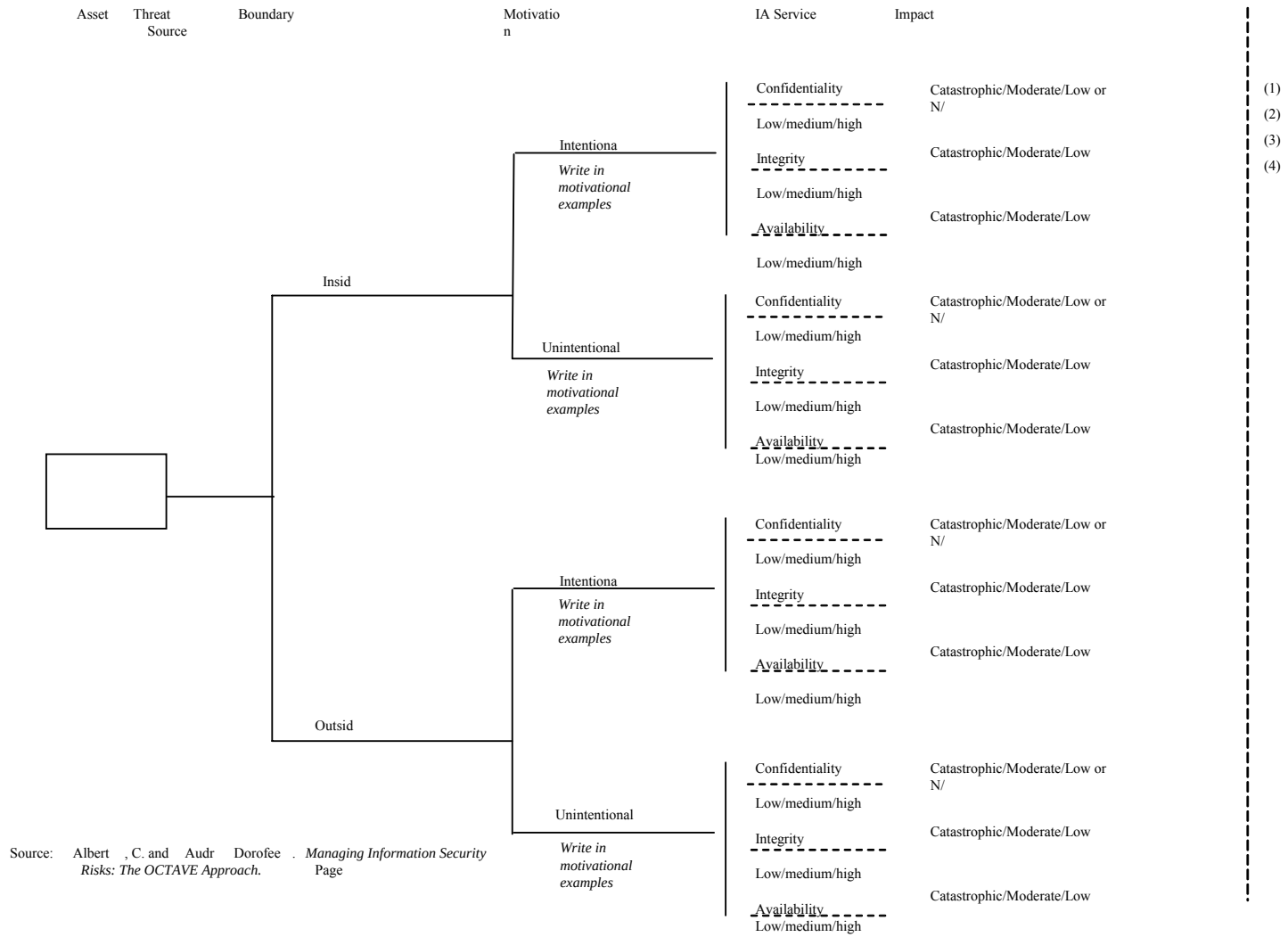


Figure 1. Asset Analysis

Figure 1 is a Risk Assessment Worksheet that should help the team to identify potential threat sources and impacts to the assets. It is important that these worksheets be retained as a historical document to help determine the rationale for the specific threats and to help with future iterations of the RAM. Building on this information is vital to the entire RAM process.



Source: Albert , C. and Audr Dorofee . *Managing Information Security Risks: The OCTAVE Approach.* Page

Figure 2. Risk Assessment Worksheet

An explanation of the risk assessment worksheet (Figure 2) is provided below.

The empty box represents the asset (for example, firewall, server, user, and so forth).

Threat Sources — Threats use threat sources as its vehicle to move through the vulnerability, reaching the asset. Categorizations of threat sources include manmade, natural, and environmental.

Man-made threat sources, as the name implies, come from people. They can be malicious, intentional, or unintentional. They can be internal to the organization, or external of the organization. External threat sources receive most of the attention, and get many of resources allocated for defending the network, at the risk of forgetting that internal threat sources are many times more threatening than external threat sources.

The network's Demilitarized Zone (DMZ) and Intrusion Detection System (IDS) are examples of highly expensive resources allocated toward protecting the network's borders. There are teams dedicated to monitor these devices, reporting their activity to management, and ensuring that their configuration is tightly controlled. These procedures are in place to protect the network; however, few allocated resources measure the standard workstation configuration and report non-compliance, increasing the vulnerability of the entire network.

Natural threat sources include fires, floods, hurricanes, or tornadoes. Prominent natural threat sources for the area includes hurricanes, windstorms, snowstorms, iced power lines, or hazardous road conditions due to icing and heavy rain downpours. Natural threat sources may not directly harm the availability of an asset by causing a power outage, but they can prevent essential personnel from arriving at a given location due to hazardous conditions.

Threat Source Identification (See Table 2-3) is the process of identifying the potential threat sources to the assets to help compile the threat statement that lists the potential threat sources capable of affecting the system. Common threat sources can be natural, human, or environmental (See Table 2.). In assessing threat sources, it is important to consider all potential threat sources that could cause harm to a system and its processing environment. For example, although the threat statement for a system located in a desert may not include “natural flood” because of the low likelihood of such an event’s occurring, environmental threats such as a bursting pipe can quickly flood a computer room and cause damage to an organization’s assets and resources. Humans can be threat sources through intentional acts, such as deliberate attacks by malicious persons or disgruntled employees, or unintentional acts, such as negligence and errors.
A deliberate attack can be one of the following:

- A malicious attempt to gain unauthorized access to a system (for example, by guessing passwords) in order to compromise system and data integrity, availability, or confidentiality (One example of this latter type of deliberate attack is a programmer’s writing a Trojan horse program to bypass system security.)

- A benign, but nonetheless purposeful, attempt to circumvent system security in order to "get the job done."

Boundary — Boundaries describe how the threat source is approaching the asset. With the exception of natural disasters, boundaries can be internal (inside), external (outside), or both. Natural disasters will always be external.

Threat Source Boundaries — A threat source must operate through a boundary, or medium, in relation to the enterprise. The threat source has two possible mediums for attack; they can be internal (inside) to the enterprise, or external (outside) to the enterprise.

Inside Boundary — Characterized as within the enterprise, an inside boundary's medium typically does not cross the demilitarized zone (DMZ) or other layers of defense used to protect the trusted information system. The internal boundary includes any of the security domains established within the overall boundary of the information system. For example, a malcontent wanting to harm to the information system while using an approved workstation is an example of an internal threat source. Internal threat sources, intentional or unintentional, are the biggest threat to the system.

Outside Boundary — Characterized as outside entity from the enterprise, an external boundary's medium typically penetrates the boundaries of the information system through the DMZ or bypasses the layers of defense protecting the information system. For example, an authorized user accesses an untrusted Web site, executing an infected ActiveX component onto the user's workstation, bypassing and penetrating the normal defenses of the information system. Table 3 provides examples of inside and outside threat sources.

Table 3. Inside and Outside Threat Sources

Threat Type	Threat Source
Inside Threats	▪ Data corruption ▪ Elevated user privileges ▪ Unauthorized software downloading ▪ No data back-up ▪ Loss of power ▪ Disgruntled employee
Outside Threats	▪ Malicious coding ▪ Password sniffing ▪ Downloading of spyware ▪ Data destruction ▪ Natural Disasters (hurricanes, flooding) ▪ Terrorists acts

Motivation — Motivation describes the intention or the threat sources' action – intentional or unintentional. It says why the threat source is acting. Understanding motivation helps to target the control or countermeasure, and thereby help reduce cost and increase the control's effectiveness. The below scenarios provide an example of the effectiveness of targeted controls.
Scenario #1: Daily IDS reports identify a particular user downloading unauthorized software, and the motivation behind the threat source's action is unintentional. The user had no knowledge that he or she was downloading a particular malicious code during routine, and authorized, Web surfing.

> **Action:** This scenario indicates that the person had no knowledge of the malicious downloading (unintentional motivation). A targeted investigation of the problem identified two factors: The Web site, although authorized by security policy, used ActiveX to download and execute code onto the user's workstation. This action sets off the IDS alarms, filing the daily reports.
>
> The user's browser configuration incorrectly allowed the downloading of ActiveX controls from an untrusted Web site.
>
> A targeted approach in implementing controls for scenario1 correctly identified two controls needed to prevent future incidents from occurring within the enterprise:
>
> Block port 80 at the firewall, the Web site can no longer download ActiveX controls to any workstation in the enterprise.
>
> A security policy review indicates that the browser's security setting was miss-configured, which allowed the downloading of ActiveX controls from untrusted Web sites. Changing this policy prevented future downloads of potentially malicious code through Active X; although, other dependencies still remain.

In Scenario #1, approach 1 – blocking port 80 – is the most secure with the greatest impact to user functionality. Approach 2 is less secure with greatest functionality. A detailed analysis could also indicate that user training would help decrease the likelihood of attack. A detailed approach is almost always needed, keeping in mind that simplicity is always best.

Scenario #2: a few days latter, the same user continues to trigger similar incidents of downloading unauthorized software. Pronounced intentional by system auditing and evidence of the same aggravated behavior, controls measures now target administrative measures, like suspending the user's Internet access or taking the matter up with management.

In both scenarios above, identifying the motivation behind the threat sources action helped increase the control's effectiveness and reduce the cost associated with the control. It would not have been productive to suspend the user's Internet access when the motivation was unintentional. Conversely, continued training to an intentional and harmful action will not stop future occurrences.

Motivation and the resources for carrying out an attack make humans potentially dangerous threat sources. Table 4 presents an overview of many of today's common human threats, their

possible motivations, and the methods or threat actions by which they might carry out an attack. This information will be useful to organizations studying their human threat environments and customizing their human threat statements. In addition, reviews of the history of system break-ins; security violation reports; incident reports; and interviews with the system administrators, help desk personnel, and user community during information gathering will help identify human threat sources that have the potential to harm a system and its data that may be a concern where a vulnerability exists.

Defining these qualities lead to the remediation or mitigation strategies necessary to reduce the vulnerabilities associated with the potential threats used to launch a successful attack on the information system.

With remediation and mitigation procedures exhausted through a systematic review of the findings, and of application of the NAP 14.2-C security controls, the DAA accepts the level of risk by being presented a C&A package by signing an Authority to Operate (ATO) or Interim Authority to Operated (IATO) for the information system.
An analysis of the motivation, resources, and capabilities that may be required to carry out a successful attack should be developed after the potential threat sources have been identified, in order to determine the likelihood of a threat's exercising a system vulnerability, as described in The Likelihood Determinations section.

Table 4 identifies and describes these potential human treat sources, motivations, threat sources, and threat actions.

Table 4. Human Threat Factors

Threat Source	Motivation	Threat Actions
Hacker, Cracker	Challenge Ego Rebellion	▪ Hacking ▪ Social engineering ▪ System intrusion, break-ins ▪ Unauthorized system access
Computer Criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data aberration	▪ Computer crime ▪ (cyber stalking) ▪ Fraudulent act ▪ (replay, impersonation, interception) ▪ Information bribery ▪ Spoofing ▪ System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	▪ Bomb or Terrorism ▪ Information warfare ▪ System attack ▪ (distributed denial of service) ▪ System penetration ▪ System tampering
Industrial Espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	▪ Economic exploitation ▪ Information theft ▪ Intrusion on personal privacy ▪ Social engineering ▪ System penetration ▪ Unauthorized system access (access to classified, proprietary, or technology-related information)

The threat statement, or the list of potential threat sources, should be tailored to the individual organization and its processing environment (for example, end-user computing habits). In general, information on natural threats (for example, floods, earthquakes, storms) should be readily available. Known threats have been identified by many government and private sector organizations. Intrusion detection tools also are becoming more prevalent, and government and industry organizations continually collect data on security events, thereby improving the ability to realistically assess threats.

Sources of information include, but are not limited to, the following:

- Intelligence agencies (for example, the Federal Bureau of Investigation's National Infrastructure Protection Center, at the DHS.
- United States Computer Emergency Readiness Team (US-CERT)
- Mass media, particularly Web-based resources such as SecurityFocus.com
- SecurityWatch.com, SecurityPortal.com, and SANS.org

2.3 Vulnerability Identification

Step 3 is the identification and analysis of the vulnerabilities associated with the system environment, in keeping with an asset-based threat assessment. The goal of this step is to develop a list of asset-based vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat sources. Table 5 presents examples of vulnerability/threat pairs.

Table 5. Vulnerability/Threat Pairs

Vulnerability	Threat Source	Threat Action
Terminate employees' system identities (ID) are not removed from the system	Terminated employees	Dialing into the network and accessing proprietary data
Firewall allows inbound telnet and **guest ID** is enabled on XYZ server	Unauthorized users (hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the **guest ID**
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system	Unauthorized users (hackers, terminated employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities

Recommended methods for identifying system vulnerabilities include the use of vulnerability sources, the performance of system security testing, and the development and manual review of a security requirements checklist. It should be noted that the types of vulnerabilities that will exist, and the methodology needed to determine whether the vulnerabilities are present, will usually vary depending on the nature of the system and the phase it is in, in the SDLC:

- If the system has not yet been designed, the search for vulnerabilities should focus on the organization's security policies, planned security procedures, system requirement definitions, and the vendors' or developers' security product analyses (for example, white papers). If the system is being implemented, the identification of vulnerabilities should be expanded to include more specific information, such as the planned security features described in the security design documentation and the results of system certification test and evaluation.

- If the system is operational, the process of identifying vulnerabilities should include an analysis of the system security features and the security controls, technical and procedural, used to protect the system.

Conduct vulnerability identification through the use of tools (that is, questionnaires, interviews, worksheets, and so forth). The uses of automated vulnerability assessment engines are also apportioned against the technology. This is discussed in the system test and evaluation (STE) process (NAP 14.2-C.)

Step 3.a: Map the enterprise

A network topology map is crucial to understanding the protection measures needed. This diagram should include critical infrastructure components, such as firewalls, IDSs, routers, switches, servers, host workstations, remote access components, storage devices, and laptops, and so forth

Step 3.b. Determine asset to tool mapping evaluation approach.

The purpose of this step is to determine potential vulnerabilities in design, implementation, or configuration of the critical assets identified in the previous steps.
Design vulnerabilities are inherent in the product.

Example: A software's control against overloading is undetermined

Implementation vulnerabilities results when execution errors exist with the product. Alarms in an intrusion detection system (IDS) go unanswered, for example. Configuration vulnerabilities results when design or administrative errors occur.

Table 6 below depicts an example of the output of the assets and tool mapping results. In addition, NAP 14.2-C will assist in determining checklist creation and determination.

Table 6. Asset Mapping Results

Asset	Automated Tool	Worksheet
Windows Server 2003	Windows Gold Disk	—
Account Creation	—	1.2.3 (example)

Note: The information contained in this table is for illustration purposes only.

Step 3.c. Categorize vulnerabilities depicted in the automated tool against the requirement

Automated tools will depict open, closed, unknown ports, or other vulnerabilities against the product. A categorization of the requirement (for example, SP 800-53 Revision 1 security control or other requirement) apportions the vulnerability to the products. See Table 7.

Table 7. Asset-based Threat Table

Asset	Windows Server 2003
Vulnerability	Latest hot fixes are not applied
NAP 14.2-C Control	SI-1
Protection Measure	Apply applicable hot fixes

Note: The information contained in this table is for illustration purposes only.

Vulnerability Sources

The technical and nontechnical vulnerabilities associated with a system's processing environment can be identified by analyzing the information-gathering techniques A review of other industry sources (for example, vendor Web pages that identify system bugs and flaws) will be useful in preparing for the interviews and in developing effective questionnaires to identify vulnerabilities that may be applicable to specific systems (for example, a specific version of a specific operating system).

Documented vulnerability sources that should be considered in a thorough vulnerability analysis include, but are not limited to, the following:

- Previous risk assessment documentation of the system assessed.
- The system's audit reports, system anomaly reports, security review reports, and system test and evaluation reports.
- Vulnerability lists, such as the NIST I-CAT vulnerability database (http://icat.nist.gov).
- Security advisories, such as US-CERT and the Department of Energy's Computer Incident Advisory Capability bulletins.
- Vendor advisories.
- Commercial computer incident/emergency response teams and post lists (for example, SecurityFocus.com forum mailings).
- Computer Emergency Response Team (http://www.cert.org)
- Security Bulletins, Vulnerability Notes, or US-CERT Technical Alerts in the United States Computer Emergency Readiness Team (US-CERT) <http://www.us-cert.gov)
- Common Vulnerabilities and Exposure List (http://www.cve.mitre.org)
- System software security analyses

System Security Testing

Proactive methods, employing system testing, can be used to identify system vulnerabilities efficiently, depending on the criticality of the system and available resources (for example, allocated funds, available technology, persons with the expertise to conduct the test).
Test methods include:

- Automated vulnerability scanning tool
- ST&E
- Penetration testing

The automated vulnerability scanning tool is used to scan a group of hosts or a network for known vulnerable services (for example, system allows anonymous File Transfer Protocol [FTP], send mail relaying). However, it should be noted that some of the potential vulnerabilities identified by the automated scanning tool may not represent real vulnerabilities in the context of the system environment. For example, some of these scanning tools rate potential vulnerabilities without considering the site's environment and requirements. Some of the "vulnerabilities" flagged by the automated scanning software may actually not be vulnerable for a particular site but may be configured that way because their environment requires it. Thus, this test method may produce false positives.

ST&E is another technique that can be used in identifying system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (for example, test script, test procedures, and expected test results). The purpose of system security testing is to

test the effectiveness of the security controls of a system as they have been applied in an operational environment. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards. Penetration testing can be used to complement the review of security controls and ensure that different facets of the system are secured. Automated scanning tools may also be employed.

Penetration testing, when employed in the risk assessment process, can be used to assess a system's ability to withstand intentional attempts to circumvent system security. Its objective is to test the system from the viewpoint of a threat source and to identify potential failures in the system protection schemes. The results of these types of optional security testing will help identify a system's vulnerabilities.

Development of Security Requirements Checklist

During this step, the risk assessment personnel determine whether the security requirements stipulated for the system and collected during system characterization are being met by existing or planned security controls. Typically, the system security requirements can be presented in table form, with each requirement accompanied by an explanation of how the system's design or implementation does or does not satisfy that security control requirement.
A security requirements checklist contains the basic security standards that can be used to systematically evaluate and identify the vulnerabilities of the assets (personnel, hardware, software, and information), nonautomated procedures, processes, and information transfers associated with a given system in the following security areas:

- Management
- Operational
- Technical

Table 8 lists security criteria suggested for use in identifying a system's Vulnerabilities in each security area.

Table 8. Security Criteria

Security Area	Security Criteria
Management Security	■ Assignment of responsibilities ■ Continuity of support ■ Incident response capability ■ Periodic review of security controls ■ Personnel clearance and background investigations ■ Risk assessment ■ Security and technical training ■ Separation of duties ■ System authorization and reauthorization ■ System or application security plan
Operational Security	■ Control of air-borne contaminants (smoke, dust, chemicals) ■ Controls to ensure the quality of the electrical power supply ■ Data media access and disposal ■ External data distribution and labeling ■ Facility protection (computer room, data center, office) ■ Humidity control ■ Temperature control ■ Workstations, laptops, and stand-alone personal computers
Technical Security	■ Communications (dial-in, system interconnection, routers) ■ Cryptography ■ Discretionary access control ■ Identification and authentication ■ Intrusion detection ■ Object reuse ■ System audit

The outcome of this process is the security requirements checklist. Sources that can be used in compiling such a checklist include, but are not limited to, the following government regulatory and security directives and sources applicable to the system processing environment:

- Computer Security Act (CSA) of 1987
- Federal Information Processing Standards Publications
- Federal Information Security Management Act of 2002 (FISMA).
- Privacy Act of 1974
- System security plan of the system assessed
- The organization's security policies, guidelines, and standards
- Industry practices.

The control objectives are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy. The results of the checklist (or questionnaire) can be used as input for an evaluation of compliance and noncompliance. This process identifies system, process, and procedural weaknesses that represent potential vulnerabilities.

2.4 Analysis of Protection Measures [Controls Analysis]

The goal of Step 4 is to analyze the controls that have been implemented, or are planned for implementation, by the organization, to minimize or eliminate the likelihood (or probability) of a threat exploiting a system vulnerability. See Table 9.

Table 9. Control Vulnerabilities by Category

Category	Vulnerability	Asset
Access Control		
Audit and Accountability		
Awareness and Training		
Certification, Accreditation, and Security Assessments		
Configuration Management		
Contingency Planning		
Identification and Authentication		
Incident Response		
Maintenance		
Media Protection		
Physical & Environmental Protection		
Planning		
Personnel Security		
Risk Assessment		
System and Service Acquisition		
System and Communications Protection		
System and Information Integrity		

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment (Step 5 below), the implementation of current or planned controls must be considered. For example, a vulnerability is not likely to be exercised or the likelihood is low if there is a low level of threat source interest or capability or if there are effective security controls that can eliminate, or reduce the magnitude of, harm.

Control Methods

Security controls are categorized into technical and nontechnical methods. Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (for example, access control mechanisms, identification and authentication mechanisms, encryption methods,

intrusion detection software). Nontechnical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.

Control Categories

The control categories for both technical and nontechnical control methods can be further classified as either preventive or detective. These two subcategories are explained as follows:

- Preventive controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication.
- Detective controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.

The implementation of such controls during the risk mitigation process is the direct result of the identification of deficiencies in current or planned controls during the risk assessment process (for example, controls are not in place or controls are not properly implemented).

Control Analysis Technique

As discussed above, development of a security requirements checklist or use of an available checklist will be helpful in analyzing controls in an efficient and systematic manner. The security requirements checklist can be used to validate security noncompliance as well as compliance. Therefore, it is essential to update such checklists to reflect changes in an organization's control environment (for example, changes in security policies, methods, and requirements) to ensure the checklist's validity. The result of the control analysis is presented in Step 5 below.

2.5 Likelihood Determination

Step 5 is designed to derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment. The following governing factors must be considered:

- Threat source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls

The likelihood that a potential vulnerability could be exercised by a given threat source can be described as high, medium, or low. Table 10 on the following page describes vulnerabilities by grouped protection measures.

Table 10. Vulnerabilities by Grouped Protection Measures

Group Measures	Asset Type	Vulnerability Description	NAP 14.2-C Control	Protection Measure	Likelihood Level
Access control	Server	Guest account open	AC-2	Disable Guest Account	High
	Workstation	Regular system users have elevated privileged accounts	AC-6	Ensure principle of least privilege remains throughout all processes	High
System and communication protection	Web site	Connections to high-impact security domains exists without monitoring	SC-7	Begin audit controls and regular Website monitoring	High

Note: The information contained in this table is for illustration purposes only.

Table 11 lists the SP 800-30-defined likelihood levels.

Table 11. Likelihood Definitions

Likelihood Rating	Likelihood Definition
High	The threat source is highly motivated and sufficiently capable, and controls are ineffective to prevent the vulnerability from being exercised.
Moderate	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

2.6 Impact Analysis (14.2-C)

Because the potential impact levels for the confidentiality, integrity, and availability, security objectives may not be identical for an information system. Step 6 uses the high water mark concept to determine the impact level of the information system. Thus, a low-impact system is

defined as an information system in which all three of the security objectives are low. A moderate-impact system is an information system in which at least one of the security objectives is moderate and no security objective is high. And finally, a high-impact system is an information system in which at least one security objective is high. Once the overall impact level of the information system is determined, the minimum set of security control can be selected from the baseline controls.

The certification team must use the methodology defined below for determining the system categorization (that is, Protection Index) based on the information system boundary, identification of information group(s), and Consequence of Loss for Confidentiality. National security information is grouped (information group) based on sensitivity (classification level, category, and need-to-know). The following paragraph describes the information groups in increasing order of sensitivity (Top Secret Restricted Data considered the most sensitive). National Security Systems must be categorized based on the most sensitive information group they contain and the impact/Consequences of Loss (CoL) if the confidentiality, integrity and/or availability of the information is lost. The impact is determined through a CoL concept that ranks the perceived value of each information group in terms of confidentiality, integrity, and availability.

Consequences of Loss – Classified Information

The tables in this section describe the criteria used to determine the CoL to confidentiality, integrity, and availability for all classified information.

Table 12. Consequences of Loss of Confidentiality

Consequence of Loss	Confidentiality Description
High	Unauthorized, premature, or partial disclosure may have a grave effect on National security, Senior DOE Management, DOE, or National interests.
Moderate	Serious damage to National security will result if confidentiality is lost; Information requiring protection mandated by policy, laws, or agreements between DOE, its contractors, and other entities, such as commercial organizations or foreign Governments; Information designated as mission-essential; or Unauthorized, premature, or partial disclosure may have an adverse effect on site-level interests.
Low	Damage to National Security will result if confidentiality is lost; Information designated as sensitive by the data owner; or unauthorized, premature, or partial disclosure may have an adverse effect on organizational interests.

Table 13. Consequences of Loss of Integrity

Consequence of Loss	Integrity Description
High	Loss of integrity will have a serious effect on National-level interests or Loss of integrity will have a serious effect on confidentiality.
Moderate	A degree of integrity required for mission accomplishment, but not absolute; Bodily injury might result from loss of integrity; or Loss of integrity will have an adverse effect on organizational-level interests.
Low	Loss of integrity impacts only the missions of site- or office-level organization.

Table 14. Consequences of Loss of Availability

Consequence of Loss	Availability Description
High	Loss of life might result from loss of availability; Information must always be available upon request, with no tolerance for delay; Loss of availability will have an adverse effect on National-level interests; Federal requirement (that is, requirement for Material Control and Accountability (MC&A) inventory); or Loss of availability will have an adverse effect on confidentiality.
Moderate	Information must be readily available with minimum tolerance for delay; Bodily injury might result from loss of availability; or Loss of availability will have an adverse effect on organizational-level interests.
Low	Information must be available with flexible tolerance for delay.

Note: In this context, “High – no tolerance for delay” means no delay;” “Moderate – minimum tolerance for delay" means a delay of seconds to hours;” and “Low – flexible tolerance for delay” means a delay of days to weeks

Table 15 provides the results of the evaluation of impact of loss for each National Security information group and represents the minimum Consequences of Lost (CoL) of value for each information group.

Table 15. Consequences of Loss of Confidentiality, Integrity, and Availability

Information Group	Loss of Confidentiality	Loss of Integrity	Loss of Availability
Confidential and Secret Information*	Moderate	Low	Low
Secret** and Top Secret Information	High	Low	Low

* Includes SRD, Sigmas 1, 2, 3, 4, 5, 9, 10, 11, 12, 13, and 15

** includes SRD, Sigmas 14 and 20

1 Sigmas 6, 7, and 8 are not currently in use. Note: the levels in this table are the minimum values allowed by NNSA. Senior NNSA management or the operating unit may assign a higher level of consequence for any or all of the information groups.

The output of this step is displayed in Step 7.

2.7 Risk Determination

The purpose of Step 7 is to assess the level of risk to the system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of:

- The likelihood of a given threat source's attempting to exercise a given vulnerability.
- The magnitude of the impact should a threat source successfully exercise vulnerability.
- The adequacy of planned or existing security controls for reducing or eliminating risk.

To measure risk, a risk scale and a risk-level matrix must be developed. The following page provides a standard risk-level matrix, and describes the resulting risk levels.

Risk-Level Matrix

The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (for example, probability) and threat impact. Table 16 shows how the overall risk ratings might be determined based on inputs from the threat likelihood and threat impact categories. This matrix below a 3 x 3 matrix of threat likelihood (High, Medium, and Low), and threat impact (High, Medium, and Low). Depending on the site's requirements and the granularity of risk assessment desired, some sites may use a 4 x 4 or a 5 x 5 matrix. The latter can include a Very Low or Very High threat likelihood and a Very Low or Very High threat impact to generate a Very Low or Very High risk level. A Very High risk level may require possible system shutdown or stopping of all system integration and testing efforts.

The risk determination process uses the likelihood and impact assessments performed in the previous two steps and attempts to assign a determination factor. The determination factor uses a weighted high, medium, and low categorization (defined below), and attempts to assign a quantitative measurement to the level of risk based on a predetermined formula. The sample matrix in Table 16 shows how the overall risk levels of High, Medium, and Low are derived.

Table 16. Risk-Level Matrix

Threat Likelihood (Step 5)	Threat Impact (Step 6)		
	Low (10)	**Medium (50)**	**High (100)**
High (1.0)	Low 10 x 1.0 = 10	Medium 50 x 1.0 = 50	High 100 x 1.0 = 100
Medium (0.5)	Low 10 x 0.5 = 5	Medium 50 x 0.5 = 25	High 100 x 0.5 = 50
Low (0.1)	Low 10 x 0.1= 1	Medium 50 x 0.1 = 5	High 100 x 0.1 = 10

Note: The information contained in this table is for illustration purposes only.

Given the values of Threat Likelihood and Threat Impact, the Risk Determination for each threat can proceed, as shown in Table 17.

Table 17. Vulnerability Risk Table

Asset Type	Vulnerability Description	NAP 14.1-C Security Control	Threat Likelihood	Threat Impact	Risk Determination Value
Windows OS	Latest hot fixes not applied	SI-1	High (1.0)	High (100)	High (100 x 1.0 = 100)
Workstation	Multiple users use the same password	IA-2	High (1.0)	Medium (50)	Medium (50 x 1.0 = 50)

Note: The information contained in this table is for illustration purposes only.

Description of Risk Level

Table 18 describes the risk levels shown in the above matrix.

Table 18. Risk Scale and Necessary Actions

Risk Rating	Action Implementation
High	High-risk levels create a strong need for corrective actions and the creation of an action plan that is put in place as quickly as possible.
	Moderate-risk levels warrant corrective actions and a plan to incorporate those actions within a reasonable period of time.
Low	For low-risk levels, the application owner must decide whether corrective actions are needed or whether the risks may be accepted.

This risk scale, with its ratings of High, Medium, and Low, represents the degree or level of risk to which a system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

2.8 Protection Requirement Recommendations

This topic describes the protection requirement recommendations (control recommendations). During Step 8 of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the system and its data to an acceptable level.

The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Existence and effectiveness of current controls
- Effectiveness of recommended options (for example, system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability

The control recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented. It should be noted that not all possible recommended controls can be implemented to reduce loss. To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. In addition, the operational impact (for example, effect on system performance) and feasibility (for example, technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully during the risk mitigation process.

2.9 Results Documentation

Once the risk assessment has been completed (threat sources and vulnerabilities identified, risks assessed, and recommended controls provided), Step 9 requires that the results of the risk assessment be documented in an official report or briefing.

Table 19 provides a sample Risk Assessment Report Vulnerability Summary table.

Table 19. Sample Risk Assessment Report Vulnerability Summary

Asset Type	Vulnerability Description	Threat Source	NAP 14.1-C Security Control	Threat Likelihood (L)	Threat Impact (I)	Risk Determination Value (L*I = Risk)	Risk Determination Value (L*I = Risk)
Windows OS	Latest hot fixes not applied	External cracker	SI-1	High (1.0)	High (100)	High (100 x 1.0 = 100)	Apply relevant software updates
Database	Multiple users use the same password	Agency employee	IA-2	High (1.0	Medium (50)	Medium (50 x 1.0 = 50)	▪ Ensure each user has a unique password ▪ Run password cracking tool set

Note: The information contained in this table is for illustration purposes only.

This page intentionally left blank.

CHAPTER III. RISK ASSESSMENT REPORT

A Risk assessment report is prepared that describes the system threats and vulnerabilities, measures the risk, and provides recommendations for control implementation. A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes.
A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes. Unlike an audit or investigation report, which looks for wrongdoing, a risk assessment report should not be presented in an accusatory manner but as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses. For this reason, some people prefer to address the threat/vulnerability pairs as observations instead of findings in the risk assessment report.

This page intentionally left blank.

APPENDIX A: ACRONYMS

The list contains acronyms used in conjunction with security assessments.

ATO	Authority to Operate
C&A	Certification and Accreditation
CoL	Consequence of Loss
DMZ	Demilitarized Zone
US-CERT	United States Computer Emergency Readiness Team (US-CERT)
FISMA	Federal Information Security Management Act
IATO	Interim Authority to Operate
IDS	Intrusion Detection System
MC&A	Material Control and Accountability
RAM	Risk Assessment Methodology
SDLC	System Development Life Cycle
STE	System Test and Evaluation
US-CERT	United States Computer Emergency Readiness Team

This page intentionally left blank.

APPENDIX B: RISK ASSESSMENT QUESTIONNAIRE

Figure B-1 shows a sample Risk Assessment Questionnaire. Notice that this questionnaire is only a suggested approach to preparing a questionnaire and that variations will depend upon actual system environments and operational restraints.

Senior Management Survey			
Process	**Is this a process used by your organization?**		
Vulnerability Management			
Is there is a documented set of procedures for managing vulnerabilities, including: ▪ Selecting vulnerability evaluation tools, checklists, and scripts ▪ Keeping up to date with known vulnerability types and attack methods ▪ Reviewing sources of information on vulnerability announcements, security alerts, and notices ▪ Identifying infrastructure components to be evaluated ▪ Scheduling of vulnerability evaluations	**Yes**	**No**	**Don't Know**
Are vulnerability management procedures followed, and are they periodically reviewed and updated?	**Yes**	**No**	**Don't Know**
Are technology vulnerability assessments performed on a periodic basis, and are vulnerabilities addressed when they are identified?	**Yes**	**No**	**Don't Know**

Figure B-1. Sample Risk Assessment Questionnaire

APPENDIX C: RISK ASSESSMENT SAMPLE QUESTIONS

This appendix provides sample interview question for a Risk Assessment Interview. Questions should be tailored based upon where the system assessed is in the system development lifecycle (SDLC). Suggested questions to be asked during interviews with site personnel are designed to obtain a good understanding of the operational and security profile characteristics of a system may include the following:

- Safety and reliability?
- Who are valid system users?
- What is the mission of the user organization?
- What is the purpose of the system in relation to the mission?
- How important is the system to the user organization's mission?
- What is the system-availability requirement?
- What information (both incoming and outgoing) is required by the organization?
- What information is generated by, consumed by, processed on, stored in, and retrieved by the system?
- How important is the information to the user organization’s mission?
- What are the paths of information flow?
- What types of information are processed by and stored on the system (for example, financial, personnel, research and development, medical, command and control)?
- What is the sensitivity (or classification) level of the information?
- What SUI categories of information are used in the system?
- What information handled by or about the system should not be disclosed and to whom?
- Where specifically is the information processed and stored?
- What are the types of information storage?

This page intentionally left blank.

APPPENDIX D: REFERENCES

This appendix lists the references used in this document.

Campbell, P. & Jason Stamp. *Classification Scheme for Risk Assessment Methods*. 2004.

Alberts, C, A. Dorofee, and J. Allen. OCTAVE Catalog of Practices, Version 2.0.

Carnegie Mellon, Software Engineering Institute. Oct 2001.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal*

Information Systems. Department of Commerce. May 2004.

NIST SP 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*. Department of Commerce. Dec 2006.

APPENDIX I: SAMPLE MEMORANDUM OF UNDERSTANDING (MOU)

SAMPLE MEMORANDUM OF UNDERSTANDING (MOU)

SUPERSEDES: (None or document title and date)

INTRODUCTION

The purpose of this memorandum is to establish a management agreement between "Organization A" and "Organization B" regarding the development, management, operation, and security of a connection between "System A," owned by Organization A, and "System B," owned by Organization B. This agreement will govern the relationship between Organization A and Organization B, including designated managerial and technical staff, in the absence of a common management authority.

AUTHORITY

The authority for this agreement is based on Interim Policy Letter XXX, NNSA Inter-site Network Interconnection Approval Process, Approval Authority, and Connection Requirements.

BACKGROUND

It is the intent of both parties to this agreement to interconnect the following information technology (IT) systems to exchange data between "ABC database" and "XYZ database." Organization A requires the use of Organization B's ABC database, and Organization B requires the use of Organization A's XYZ database. The expected benefit of the interconnection is to expedite the processing of data associated with "Project R" within prescribed timelines.

Each IT system is described as follows:

SYSTEM A

- Name
- Function
- Location
- Description of data, including sensitivity or classification level

SYSTEM B

- Name
- Function
- Location
- Description of data, including sensitivity or classification level

COMMUNICATIONS

Frequent formal communications are essential to ensure the successful management and operation of the interconnection. The parties agree to maintain open lines of communication between designated staff at both the managerial and technical levels. All communications described herein must be conducted in writing unless otherwise noted.

The owners of System A and System B agree to designate and provide contact information for technical leads for their respective system, and to facilitate direct contacts between technical leads to support the management and operation of the interconnection to include establishing cross-domain accounts. To safeguard the confidentiality, integrity, and availability of the connected systems and the data they store, process, and transmit, the parties agree to provide notice of specific events within the time frames indicated as follows:

SECURITY INCIDENTS: Technical staff will immediately notify their designated counterparts by telephone or e-mail when a security incident(s) is detected, so the other party may take steps to determine whether its system has been compromised and to take appropriate security precautions. All NNSA security incidents will be reported to the IARC in accordance with incident reporting procedures defined in 14.1-C, *NNSA Baseline Cyber Security Program*.

DISASTERS AND OTHER CONTINGENCIES: Technical staff will immediately notify their designated counterparts by telephone or e-mail in the event of a disaster or other contingency that disrupts the normal operation of one or both of the connected systems. Additional contingency procedures must comply with the contingency plan or approved procedures as dictated by the applicable Information System Security Plan (ISSP).

AUDIT TRAIL RESPONSIBILITIES: Both parties are responsible for auditing application processes and user activities involving the interconnection. Activities that will be recorded include event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. Audit logs will be retained for one (1) year. Both parties must also *monitor* user activity to ensure that NNSA information systems are used for official purposes only.

MATERIAL CHANGES TO SYSTEM CONFIGURATION: Planned technical changes to the system architecture will be reported to technical staff before such changes are implemented. The initiating party agrees to conduct a risk assessment based on the new system architecture and to modify and re-sign the ISA within one (1) month of implementation.

NEW INTERCONNECTIONS: The initiating party will notify the other party at least one (1) month before it connects its information system with any other information system, including systems that are owned and operated by third parties.

PERSONNEL CHANGES: The parties agree to provide notification of the separation or long-term absence of their respective system owner or technical lead. In addition, both parties will provide notification of any changes in point of contact information. Both parties also will provide notification of changes to user profiles, including users who resign or change job responsibilities.

APPENDIX J: SAMPLE NNSA INTERCONNECTION SECURITY AGREEMENT

SAMPLE NNSA INTERCONNECTION SECURITY AGREEMENT

PARAGRAPH1: INTERCONNECTION STATEMENT OF REQUIREMENTS

The requirements for interconnection between “Organization A” and “Organization B” are for the express purpose of exchanging data between “System A,” owned by Organization A, and "System B," owned by Organization B. Organization B requires the use of Organization A's "XYZ database" and Organization A requires the use of Organization B's "ABC database." The expected benefit is to expedite the processing of data associated with "Project R" within prescribed timelines. The following individuals are the primary points of contact for System A and System B. [Insert listing of responsible individuals with phone numbers and e-mail addresses.]

For additional system security specifics and operational requirements for the referenced interconnected systems, refer to the applicable Information System Security Plan (ISSP) governing each system.

This Interconnection Security Agreement (ISA) is referenced in the applicable Memorandum of Understanding (MOU) governing this interconnection.

PARAGRAPH2: SYSTEM SECURITY CONSIDERATIONS

General Information/Data Description. The interconnection between System A, owned by Organization A, and System B, owned by Organization B, is a two-way path. The purpose of the interconnection is to deliver the XYZ database to Organization B's Data Analysis Department and to deliver the ABC database to Organization A's Research Office.

Services Offered. No user services are offered. This connection only exchanges data between Organization A's system and Organization B's system via a dedicated in-house connection.

Data Sensitivity. The sensitivity of data exchanged between Organization A and Organization B is Unclassified Mandatory Protection/Sensitive Unclassified Information.

User Community. All Organization A users with access to the data received from Organization B are U.S. citizens with a valid and current Organization A background investigation. All Organization B users with access to the data received from Organization A are U.S. citizens with a valid and current Organization B background investigation.

Information Exchange Security. The security of the information being passed on this two-way connection is protected through the use of FIPS 140-2 approved encryption mechanisms. The connections at each end are located within controlled access facilities, guarded 24 hours a day. Individual users will not have access to the data except through their systems security software inherent to the operating system. All access is controlled by authentication methods to validate the approved users.

Trusted Behavior Expectations. Organization A's system and users are expected to protect Organization B’s ABC database, and Organization B's system and users are expected to protect Organization A’s XYZ database, in accordance with the Privacy Act and Trade Secrets Act (18 U.S. Code 1905) and the Unauthorized Access Act (18 U.S. Code 2701 and 2710).

Telecommunication Requirements. Telecommunication methods [e.g., cabling, Protected Transmission System or (PTS), labeling of conduit, etc.] are implemented in accordance with site-specific telecommunication requirements. For additional information, reference [Insert proper name of site-specific telecommunication policy.]

Enclave Protection Requirements. Both parties are responsible for maintaining a firewall that limits network traffic to only those known ports and services described in the ISA. Both parties will also maintain their own Intrusion Detection System (IDS).

Compliance Deviations. All NNSA, DOE, and other known requirements have been met with the exception of the following approved deviations:

[Insert list of deviations with approval dates and agents.]

Configuration Management Requirements. Both parties are responsible for complying with configuration management requirements as dictated by the applicable ISSP. Each organization is required to notify the appropriate points of contact if configuration changes are being considered so that a security significance determination can be made by all affected parties.

PARAGRAPH 3: TOPOLOGICAL DRAWING

[Insert a drawing here.]

PARAGRAPH 4: SIGNATORY AUTHORITY

This ISA is valid for one (1) year after the last date on either signature below. At that time it will be updated, reviewed, and reauthorized. Either party may terminate this agreement upon 30 days' advanced notice in writing or in the event of a security incident that necessitates an immediate response.

(Organization A Official) **(Organization B Official)**

_____ _____