NNSA POLICY LETTER

NAP 14.2-C

Approved: 05-02-08

NNSA CERTIFICATION AND ACCREDITATION (C&A) PROCESS FOR INFORMATION SYSTEMS

NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of Chief Information Officer

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

INITIATED BY:
Office of the Chief Information Officer

This page left intentionally blank.

Table of Contents

CHAPTER I: NNSA CERTIFICATION AND ACCREDITATION (C&A) PROCESS I-1

1. PURPOSE I-1
2. CANCELLATIONS I-1
3. APPLICABILITY I-1
4. BACKGROUND I-3
5. REQUIREMENTS I-3
6. RESPONSIBILITIES I-5
7. DEFINITIONS I-5
8. CONTACT I-5

CHAPTER II: CONTRACTOR REQUIREMENTS DOCUMENT II-1

1. REQUIREMENTS II-1

CHAPTER III: CERTIFICATION AND ACCREDITATION (C&A) PROCESS III-1

1. INTRODUCTION III-2
3. CERTIFICATION AND ACCREDITATION PROCESS III-5
3. SECURITY CONTROL MONITORING III-17

CHAPTER IV: NNSA MANAGEMENT, OPERATIONAL, AND TECHNICAL CONTROLS IV-1

CHAPTER V: SECURITY CATEGORY V-1

CHAPTER VI: INFORMATION SYSTEM SECURITY PLAN AND ACCREDITATION PACKAGE VI-1

1. REQUIREMENTS VI-1
2. INFORMATION SYSTEM SECURITY PLAN VI-1
3. ISSP CONTENTS VI-3

CHAPTER VII: PROTECTION REQUIREMENTS FOR SENSITIVE UNCLASSIFIED INFORMATION (SUI) VII-1

1. INTRODUCTION VII-1
2. CRITERIA AND PROCESSES VII-1
3. REMOTE ACCESS VII-2
4. MANAGEMENT OF PII ON PORTABLE/MOBILE DEVICES AND REMOVABLE MEDIA VII-2

Figures

FIGURE III-1. PHASE 1 CHECKLIST 12
FIGURE III-2. VERIFICATION PACKAGE CONTENTS 15
FIGURE III-3. PHASE 3 CHECKLIST 16
FIGURE III-4. PHASE 4 CHECKLIST 18

Tables

TABLE III-1. COL OF CONFIDENTIALITY 7
TABLE III-2. COL OF INTEGRITY 7
TABLE III-3. COL OF AVAILABILITY 7
TABLE III-4. COL OF CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY 8
TABLE III-5. POTENTIAL IMPACT FOR CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY 8
TABLE III-6. LEVELS OF CONCERN FOR UNCLASSIFIED INFORMATION 9

Appendices

APPENDIX A: ACRONYMS A-1
APPENDIX B: GLOSSARY B-1

This page left intentionally blank.

CHAPTER I: NNSA CERTIFICATION AND ACCREDITATION PROCESS

1. PURPOSE. Establish requirements for a NNSA Certification and Accreditation (C&A) process that incorporates national level requirements and applies them consistently across all NNSA elements.

2. CANCELLATIONS. This NNSA Policy replaces NAPs 14.3A, 14.4A, 14.5A, 14.6A, 14.7A, 14.8A, 14.9A, 14.10A, 14.11A, 14.14, and 14.15.

3. APPLICABILITY. This NNSA Policy Letter (NAP) applies to all NNSA entities, Federal and contractor, that collect, create, process, transmit, store, and disseminate information on automated information systems for NNSA.

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

   b. Scope. This NAP applies to any information system that collects, creates, processes, transmits, stores, and disseminates unclassified or classified NNSA data. This NAP applies to any information system life cycle, 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 mean any resource that is used to collect, create, process, transmit, store, or disseminate data owned by, for, or on behalf of NNSA or DOE, as determined by the cognizant DAA.

   c. Deviations. Deviations from the requirements prescribed in this NAP must be processed as described in NAP 14.1-C, *NNSA Baseline Cyber Security Program.*

   d. 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 policy for activities under the Deputy Administrators cognizance.

      (2) These requirements do not apply to systems processing Sensitive Compartmented Information (SCI) located at NNSA sites. SCI must be protected in accordance with the appropriate intelligence community policies and directives.

e. Site/Facility Management Contractors. Except for the exclusions in paragraph 3d, the Contractor Requirements Document (CRD), Chapter II, sets forth requirements of this policy that will apply to site/facility management contractors whose contracts include the CRD.

The CRD must be included in site/facility management contracts that provide automated access to NNSA information or information systems.

The CRD does not automatically apply other than site/facility management contractors. Any application of requirements of this policy to other than site/facility management contractors will be communicated separately.

As the laws, regulations, and DOE and NNSA directives clause of site/facility management contracts states, regardless of the performer of the work, site/facility management contractors with the CRD incorporated into their contracts are responsible for compliance with the requirements of the CRD.

Affected site/facility management contractors are responsible for flowing down the requirements of the CRD to subcontractors at any tier to the extent necessary to ensure the site/facility management contractors' compliance with the requirements.

Contractors must not flow down requirements to subcontractors unnecessarily or imprudently. That is, contractors will: –

Ensure that they and their subcontractors comply with the requirements of the CRD; and

Incur only costs that would be incurred by a prudent person in the conduct of competitive business.

f. Implementation. A plan for the implementation of this NAP must be completed within 60 days of a site's contract to include this NAP. A plan for the implementation of this NAP within an NNSA Federal organization must be completed within 60 days after issuance of this NAP. 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. This implementation plan schedule shall not exceed three years from the latest accreditation date for any system prior to the effective date of this NAP.

(1) Existing Accredited Information Systems. All current and valid information system accreditations may continue in effect until the accreditation expires or re-accreditation is necessary. Re-accreditation of these systems must conform to the NNSA C&A process outlined in this policy.

(2) Information Systems in Progress. Information systems that have begun the C&A process before release of this NAP may be accredited under the previous requirements. These systems will remain accredited until re-accreditation is required, either because the systems have passed the 3-year accreditation expiration date or because a security-significant change has been made to the information system or its environment (i.e., physical, logical, or operational). Re-accreditation must conform to the NNSA C&A process outlined in this policy.

(3) Non-Accredited Information Systems. Information systems that require initial accreditation, or re-accreditation outside of (1) and (2) above, must be certified and accredited in accordance with the NNSA C&A process outlined in this policy.

4. BACKGROUND. This NAP documents the requirements for C&A in an effort to provide a comprehensive and consistent approach to C&A for all NNSA classified and unclassified information systems. C&A is the process of identification, formal assessment (certification), acceptance (accreditation), and continued operation of system security controls that protect information systems and information stored or processed on those systems. This process encompasses the system's life cycle to assure that the risk of operating a system is recognized, evaluated, and accepted. The C&A process implements the concept of "adequate security," or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. The proper implementation of the NNSA C&A process will ensure that all applicable requirements have been integrated into the development and operational processes. All NNSA information systems must have a complete C&A prior to going operational (i.e., processing live data).

This document addresses the requirements of the DOE and NNSA to ensure that adequate security controls are provided for all information systems. Additionally, this document provides guidance for the implementation of DOE M 205.1-4. Implementing the minimum security controls of this NAP will allow NNSA cyber systems to operate at an acceptable risk level.

5. REQUIREMENTS.

a. Each General Support System (GSS) or Major Application (MA) and minor applications must be accredited or have an Interim Approval to Operate (IATO) from the Designated Approving Authority (DAA) before any NNSA information is processed, created, and/or transmitted on the system.

b. Each information system must be re-accredited at least every three years or whenever a security-significant change is to be made to the information system or its environment (i.e., physical, logical, or operational).

c. The C&A activities must comply with the procedures described in Chapter III, *NNSA C&A Process.*

d. Each information system shall be accredited using one of the following forms of accreditation.

(1) System Accreditation. An accreditation method used for a single information system operating under a single Information System Security Plan (ISSP). Accreditation is based on certification of the information system.

(2) Site Accreditation. An accreditation method used to accredit multiple instances of an information system where all instantiations (i.e., installations) of the information system are to be operated in equivalent or more stringent operational environments. The DAA may approve a Site (i.e., "Master") ISSP to cover all such information systems. The information systems covered by a Site ISSP may range from personal computers up to and including multi-user information components and local area networks that meet the criteria for a Site ISSP approach. The authority to operate additional instantiations under the ISSP is based on successful completion of the follow-on processes described in the ISSP. The DAA must accredit the first information system under the Site ISSP, and delegate subsequent accreditations. The CSSM must certify that all other individual information systems to be operated under the Site ISSP meet the conditions of the approved Master ISSP. This certification, in effect, accredits the individual information systems to operate under the Site ISSP.

(a) The information system's certification documentation must contain the information system's identification and location, and must include a statement signed by the CSSM certifying that the information system implements the requirements in the Site ISSP.

(b) All information systems certified under a Site ISSP remain certified until significant changes are made to the Site ISSP, or three years have elapsed since the information system was certified.

(3) Type Accreditation. An accreditation method used to accredit multiple connections to one network, where the connections are located at different sites but a single DAA is responsible for the entire network. Each connection must be implemented using the same ISSP. Accreditation is based on the approval of processes for testing and certifying additional connections. The authority to operate additional connections under the ISSP is based on successful completion of the follow-on processes described in the ISSP.

e. Security Test and Evaluation (ST&E) plans must be developed for each information system and each information system's controls as described by the ST&E process in Chapter IV.

f. A minimum set of security controls, as determined by the system categorization process, must be implemented on all NNSA systems to appropriately protect information.

g. The DAA must:

(1) Approve the ISSP prior to the beginning of the control assessment and updated as a result of deficiencies identified during the ST&E process.

(2) Approve the ST&E Plan prior to the start of the ST&E process.

h. Sensitive Unclassified Information (SUI), including Personally Identifiable Information (PII), must be appropriately protected as described in NAP 14.1-C, *Baseline Cyber Security Program.*

6. RESPONSIBILITIES. Roles and responsibilities for all activities in this document are described in NAP 14.1-C, *NNSA Baseline Cyber Security Program.*

7. DEFINITIONS. See NAP 14.1-C, *Baseline Cyber Security Program.*

8. CONTACT. Questions concerning this NAP should be directed through the cognizant DAA to the NNSA Cyber Security Program Manager (CSPM), at 202-586-9728.

THOMAS P. D'AGOSTINO
Administrator

This page left intentionally blank.

CHAPTER II: CONTRACTOR REQUIREMENTS DOCUMENT

This Contractor Requirements Document (CRD) establishes the requirements for NNSA contractors with access to NNSA and DOE information systems. Contractors must comply with the requirements listed in the CRD. The contractor will ensure that it and its subcontractors cost-effectively comply with the requirements of this CRD.

Regardless of the performer of the work, the contractor is responsible for complying with and flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements. In doing so, the contractor must not unnecessarily or imprudently flow down requirements to subcontractors. That is, the contractor will ensure that it and its subcontractors comply with the requirements of this CRD and incur only those costs that would be incurred by a prudent person in the conduct of competitive business.

1. REQUIREMENTS. A plan for the implementation of this NAP must be completed within 60 days after modification of the site's contract to include this CRD. 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. This implementation plan schedule shall not exceed three years from the latest accreditation date for any system prior to the effective date of this NAP.

    a. Existing Accredited Information Systems. All current and valid information system accreditations may continue in effect until the accreditation expires or re-accreditation is necessary. Re-accreditation of these systems must conform to the NNSA C&A process outlined in this policy.

    b. Information Systems in Progress. Information systems that have begun the C&A process before release of this NAP may be accredited under the previous requirements. These systems will remain accredited until re-accreditation is required, either because the systems have passed the 3-year accreditation expiration date or because a security-significant change has been made to the information system or its environment (i.e., physical, logical, or operational). Re-accreditation must conform to the NNSA C&A process outlined in this policy.

    c. Non-Accredited Information Systems. Information systems that required no previous accreditation (e.g., legacy systems) must be certified and accredited in accordance with the NNSA C&A process outlined in this policy.

2. All General Support Systems (GSSs), Major Applications (MA), and minor applications managed and/or operated by an NNSA element must be accredited or have an Interim Approval to Operate (IATO) before any information is processed, created, stored, and/or transmitted, as described in this policy.

3. All information systems managed and/or operated by an NNSA element must be re-accredited at least every three years or whenever a security-significant change is to be made to an information system or its environment (i.e., physical, logical, or operational).

4. The contractor must follow the C&A activities as described in this NAP.

5. All information systems managed and/or operated by an NNSA element shall be accredited using one of the following forms of accreditation.

   a. System accreditation. An accreditation method used for a single information system operating under a single ISSP. Accreditation is based on information system certification.

   b. Site accreditation. An accreditation method used to accredit multiple instances of an information system where all instantiations (i.e., installations) of the information system are to be operated in equivalent or more stringent operational environments. The DAA may approve a Site (i.e., "Master") ISSP to cover all such information systems. The information systems covered by a Site ISSP may range from personal computers up to and including multi-user information components and local area networks that meet the criteria for a Site ISSP approach. The authority to operate additional instantiations under the ISSP is based on successful completion of the follow-on processes described in the ISSP. The DAA must accredit the first information system under the Site ISSP. The ISSM must certify that all other individual information systems to be operated under the Site ISSP meet the conditions of the approved Site ISSP. This certification, in effect, accredits the individual information systems to operate under the Site ISSP.

      (1) The information system's certification documentation must contain the information system's identification and location, and must include a statement signed by the ISSM certifying that the information system implements the requirements in the Site ISSP.

      (2) All information systems certified under a Site ISSP remain certified until significant changes are made to the Site ISSP, or three years have elapsed since the information system was certified.

   c. Type Accreditation. An accreditation method used to accredit multiple connections to one network, where the connections are located at different sites but a single DAA is responsible for the entire network. Each connection must be implemented using the same ISSP. Accreditation is based on the approval of processes for testing and certifying additional connections. The authority to operate additional connections under the ISSP is based on successful completion of the follow-on processes described in the ISSP.

6. The accreditation decision for each information system must be supported by C&A documentation as described in Chapter III of this document.

7. The contractor must develop Security Test and Evaluation (ST&E) plans for each information system. Each information system's control implementation is assessed as described in Chapter IV.

8. A minimum set of security controls, as determined by the system categorization process, must be implemented on all NSA systems to appropriately protect information.

9. The DAA must:

   a. Approve the ISSP prior to the beginning of the control assessment and updated as a result of deficiencies identified during the ST&E process and

   b. Approve the ST&E Plan prior to the start of the ST&E process.

10. Contractor must implement the minimum set of security controls as determined by the system categorization process for each information system to appropriately protect information that is processed, and stored, on unclassified and classified information systems.

11. The contractor must appropriately protect Sensitive Unclassified Information (SUI), including Personally Identifiable Information (PII), as described in NAP 14.1-C, *NNSA Baseline Cyber Security Program*.

12. The contractor must document training requirements for all contractor personnel involved in C&A activities

This page left intentionally blank.

CHAPTER III: CERTIFICATION AND ACCREDITATION (C&A) PROCESS

National Nuclear Security Administration
(NNSA)
Office of the Chief Information Officer

1. INTRODUCTION.

This document is designed to implement applicable national-level and DOE requirements in the C&A of all NNSA systems and applications. This document is intended to provide a comprehensive and uniform approach for C&A.

Ideally, the C&A process should be integrated into the system development life cycle during the capital planning and investment control process. During development, the ISSP should be written and the initial risk assessment completed in order to provide an assessment of the possible risks to the system. Additionally, the security-related documents listed in Appendix A through C of this document must be completed as appropriate during this process.

Every NNSA system and major and minor application must have official approval to operate (ATO). This approval can consist of a formal accreditation which is valid for up to three years or until a security-significant change occurs, or the approval can be an Interim Approval to Operate (IATO), *which is only valid for a maximum of six months.* An IATO can be granted by the DAA provided DAA-approved protection measures are in place and functioning during the period of the IATO.

Scope

This document addresses the NNSA C&A process as adopted by the NNSA OCIO. Within this document, the four phases of C&A are detailed as well as supporting checklists and templates to be used during the process. This document must be used by all NNSA elements.

Outcome

The C&A methodology outlined in this document provides NNSA system owners and program managers with uniform guidance on how to their information systems are certified and accredited. Proper use of the C&A methodology will assure NNSA that the level of security implemented and controls in place adequately protect assets given an acceptable level of residual risk. NNSA will benefit from the C&A activities performed on information systems in the following ways:

- Formal approval to operate
- Standard security environment through utilization of baseline security requirements
- Clearly defined system boundaries
- Documented security plans
- Defined and tested contingency plans
- Established configuration management processes
- Heightened information security awareness

Validated security controls

Measured levels of risk based on identified threats and vulnerabilities

Defined security roles and responsibilities

Structure

This document is organized into three major sections. Section 1 introduces the NNSA C&A Process. Section 2 provides a reference to the roles and responsibilities of the key parties involved in the C&A process. Section 3 describes the C&A process. A checklist has been included at the end of each phase. These checklists are designed to provide a quick reference for all participants in the process.

Special Consideration - Interim Approval To Operate (IATO)

An IATO may be deemed necessary by the Designated Approving Authority (DAA) if there is an overarching mission need to place a new system into operation or continue processing on an existing system.

IATO Request Process

The IATO Request process is a structured approach to monitor the effectiveness of the security controls in the information system during the IATO period. Consequently, the IATO Request submitted by the ISSM is used by the authorizing official to monitor the progress of correcting any deficiencies noted during the security certification, if that was the reason for the IATO. NNSA elements must maintain a copy of the IATO approval for record keeping, as well as for forwarding to appropriate personnel upon request.

All deficiencies noted during the certification process that will be used as the basis for the IATO must be tracked in the system POA&M that is forwarded to the DAA with the IATO request. Reportable Conditions must be resolved within 180 days. Before a deficiency can be considered resolved, sites must provide their cognizant DAAs with verification documentation and formally request concurrence.

Interim Authority to Test (IATT)

Another option for interim processing is an Interim Authority to Test (IATT). If a system needs to be operational during the development phase, the DAA may approve an IATT for a maximum of six (6) months. In this case, the system developers and the DAA will agree via formal documentation as to what information groups can be processed on the system during the IATT as well as what security controls (i.e., management, operational, and technical), are temporarily required until the system can be successfully certified.

Final Accreditation

In accordance with OMB policy, an information system is not considered to have received its final accreditation during the period of IATO. When the reason for the IATO has been resolved, and any identified security-related deficiencies have been adequately addressed, the interim authorization should be lifted and the information system accredited to operate.

2. ROLES AND RESPONSIBILITIES.

The majority of roles and responsibilities for key participants in the NNSA C&A process are detailed in NAP 14.1-C, *NNSA Baseline Cyber Security Program*. Additional roles are described below.

Certification Team (CT)

The CT is responsible for conducting the certification activities. The CT is responsible for coordinating C&A activities and consolidating the final C&A package. The team will determine if the security controls are correctly implemented and effective. The CT will make this determination after receiving input from the ST&E Team.

Security Test and Evaluation (ST&E) Team

The ST&E team, whose membership must include the system's ISSO, is responsible for performing the ST&E on the system and validating that the controls on the system are present and operating in accordance with the ISSP.

The ST&E team must include one member who is independent of the system under evaluation in the sense that they should not have (a) been the developers of the system nor (b) be a privileged user of the system. In order to ensure independence and competence, the ST&E team and its technical qualifications must be approved by the Certification Agent (CA) prior to the commencement of the C&A process.

The results of the ST&E, together with the rest of the certification package, will be presented by the ISSO to the CA so that they can make an accurate determination of the risk to the system, and thus provide an informed accreditation recommendation to the DAA.

Program Manager and System Owner

The program manager (if applicable) and system owner represent the interest of the user community and the information system throughout the system's life cycle. The program manager is responsible for the system during initial development and acquisition and is concerned with cost, schedule and performance issues. The system owner assumes responsibility for the system after delivery and installation and is responsible for system operation, system maintenance, and disposal. Together they are responsible for ensuring the system is deployed and operated according to the security controls documented in the ISSP and are also responsible for seeing that system users and security support personnel receive the requisite security training.

The program manager and system owner will ensure that the C&A effort is coordinated and provide the necessary resources and information to the CT. They will ensure the preparation of the certification package before it is presented to the CA.

3. CERTIFICATION AND ACCREDITATION PROCESS.

Phase 1: Pre-Certification

Phase 1 involves gathering information about the system to be certified, determining the scope of the certification effort, validating the initial ISSP for the system (if available), performing the initial validation of the risk assessment and system security controls, and determining the C&A schedule. During phase 1, the system owner or program manager will establish the certification schedule in coordination with all appropriate stakeholders.

Step 1: Define the System and Scope of the C&A Effort

During this phase, the CT gathers all available system information (e.g., design documents, system descriptions, graphics, system plans, and approved Interconnection Security Agreement) in order to get a comprehensive system description and to define the scope of the C&A effort. Defining the system involves identifying the software, hardware, and communications equipment within the system boundary which may impact security in order to understand what needs to be examined for the C&A effort.

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.

A general support system is an interconnected set of information resources. Such 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 enter including its operating system and utilities, a tactical radio network, or a shared information processing service organization. Normally, the purpose of a general support system is to provide processing or communications support.

A major application is an information system(s) that perform clearly defined functions for which there are readily identifiable security considerations and needs (e.g., an electronic funds transfer system). A major application comprises many components (e.g., hardware, software, and telecommunications components) that provide a common functionality. Major applications require 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]. A software application alone without hardware and the supporting operating system is insufficient for consideration as an accreditation boundary. For example, a certification and accreditation Information System Security Plan (ISSP) for a major application could include a vulnerability management application, along with its supporting operating system(s) and hardware component(s).

During Phase 1 the C&A key participants (e.g., DAA, CA, the program manager, the system owner, the certification team, the CSSO, other officials in the NNSA element or department that have an interest in the system) will agree on the scope and schedule for C&A activities. The CA must approve of the ST&E team and ensure they are technically competent prior to the commencement of the rest of the C&A process.

Determine the Security/System Categorization

Since the potential impact levels for the confidentiality, integrity, and availability security objectives may not be identical for an information system, the high water mark concept is used 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 in Chapter IV..

National Security Systems

For national security systems, the certification team must use the methodology defined below for determining the system categorization (i.e., Control Baseline) based on the information system boundary, identification of information group(s), and Consequences of Loss (CoL) 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/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**.**

Tables III-1 through Table III-3 describe the criteria used to determine the CoL to confidentiality, integrity, and availability for all classified information. Table III-4 provides the results of the evaluation of impact of loss for each national security information group and represents the minimum CoL value for each information group.

Table III-1. CoL of Confidentiality

Consequences of Loss	Confidentiality
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 III-2. CoL of Integrity

Consequences of Loss	Integrity
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 III-3. CoL of Availability

Consequences of Loss	Availability
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 (i.e., 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 III-4. CoL 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. 15 and 20 are grouped as moderate.

** Includes SRD, Sigmas 14.[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 Management or the operating unit may assign a higher level of consequence for any or all of the information groups.

Unclassified Information Systems and Major Applications

To determine the security categorization for unclassified information systems and major applications, the levels of risk must first be identified for confidentiality, integrity, and availability. FIPS PUB 199 provides guidance for assigning security categorization factors for information processed on Federal systems. Each factor is assigned a level of low, moderate, or high. Confidentiality provides assurance that the system data is protected from disclosure to unauthorized personnel, processes, or devices. Integrity provides assurance that the data processed by the system is protected from unauthorized, unanticipated, or unintentional modification or destruction. Availability provides assurance that the system data and resources will be available to authorized users on a timely and reliable basis.

The format for documenting the security categorization is as follows: CATEGORIZATION = [(confidentiality, Potential Impact), (integrity, Potential Impact), (availability, Potential Impact.)]

Table III-5 below provides guidance on how to determine which risk-level of concern should be assigned to confidentiality, integrity, and availability.

Table III-5. Potential Impact for Confidentiality, Integrity, and Availability

	Risk Level		
	Low	**Moderate**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C §3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of confidentiality could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective repairs.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of confidentiality could be expected to cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.	The unauthorized disclosure of information could be expected to have a **severe** or **catastrophic** adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of confidentiality could be expected to cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.
Integrity Guarding against improper information modification, destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C. §3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of integrity could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of integrity could be expected to cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.	The unauthorized modification or destruction of information could be expected to have a **severe** or **catastrophic** adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of integrity could be expected to cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.
Availability Ensuring timely and reliable access to and	The disruption of access to information could be expected to have a limited adverse effect on agency operations (including mission,	The disruption of access to information could be expected to have a **serious** adverse effect on agency operations (including mission,	The disruption of access to information could be expected to have a **severe** or **catastrophic** adverse effect on agency operations (including

	Risk Level		
	Low	**Moderate**	**High**
use of information. [44 U.S.C. §3542]	functions, image, or reputation), agency assets, or individuals. A loss of availability could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective repairs.	functions, image, or reputation), agency assets, or individuals. A loss of availability could be expected to cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.	mission, functions, image, or reputation), agency assets, or individuals. A loss of availability could be expected to cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.

There are three information groups used to define unclassified information. They are Open, Public, Unrestricted Access; Unclassified Protected; and Unclassified Mandatory Protection. Table III-6 provides information regarding the minimum LoC for the *confidentiality* of unclassified information, along with their assigned Protection Indices. Sites are to determine the levels of concern for integrity and availability.

Table III-6. Levels of Concern for Unclassified Information

Information Group	Definition	LoC
Open, Public, Unrestricted Access	Information requires no protection from disclosure; e.g., approved for public release	Low
Unclassified Protected	Information designated as requiring protection by the data owner or data steward.	Low
Unclassified Mandatory Protection/SUI	Unclassified information requiring protection mandated by policy or laws. See NAP 14.1-C.	Moderate

Step 2: Identify Security Controls

The security controls include management, operational, assurance, and technical controls for the system, as it will be operated, as well as environmental controls and physical security controls. During this step, the minimum set (baseline) of security controls that should be present on the system are identified and documented in the ISSP. The system categorization is used to select a minimum set of security controls from Chapter IV, as appropriate. Security controls that uniquely support the confidentiality, integrity, or availability security objectives may be downgraded to the corresponding control in a lower baseline (or appropriately modified or eliminated if not defined in a lower baseline) if, and only if the downgrading action: (i) is consistent with the security categorization for the corresponding security objectives of confidentiality, integrity, or availability before moving to the high water mark; (ii) is supported

by an organizational assessment of risk; and (iii) does not affect the security-relevant information within the information system.

The following security controls are potential (although not all-inclusive) candidates for downgrading: (i) for confidentiality [AC-15, MA-3 (3), MP-3, MP-6, PE-5, SC-4, SC-9]; (ii) for integrity [SC-8]; and (iii) for availability [CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, MA-6, PE-9, PE-10, PE-11, PE-13, PE-15, SC-6].

A risk review of the security physical, logical, and operational environment is conducted to identify any system or site unique threats/ vulnerabilities as well as identify any operational security practices required by the system owner/ data owner/ steward. Adjustments are made to the minimum set of security controls by identifying additional/ new security controls that will mitigate those threats/ vulnerabilities and/or implement the operational practices required by the system owner/ data owner/ steward. These additional controls may be selected (and modified as needed) from the security controls in Chapter IV, or new security controls may be created to satisfy these additional requirements.

Additionally, system privacy implications are reviewed to include preparation of a Privacy Impact Assessment (PIA) **for externally facing (publicly accessible) systems that contain privacy information** and additional requirements needed to secure the system at the proper security/system categorization.

Step 3: Conduct a Privacy Impact Assessment (PIA) if required

If a PIA is required, it must be completed as detailed in “DOE Procedures for Conducting Privacy Impact Assessments”. A PIA is required whenever the system contains data covered under the Privacy Act of 1974 (Public Law 93-579), September, 1975, if the system is external facing.

Step 4: Review the ISSP

The ISSP provides a system description, a list of the security requirements for the system, and explains how the system security controls are implemented. The initial ISSP should be created during system development as part of the security requirements definition for the system. ISSPs should be updated whenever changes are made to the security posture of the system. See Chapter V for an outline of the ISSPs required contents.

During this step, the existing ISSP should be reviewed by the system owner and CT to ensure that it describes the security controls required for the system. The CT will also verify that the control implementations described are appropriate for the security/system categorization and that the ISSP provides information about any user organizations, both internal and external, that connect to the system. If the system does interconnect with other systems or organizations not under the operational control of the sponsoring organization, details about the security controls on those connections shall be documented in an Interconnection Security Agreement (ISA).

Step 5: Review the Initial Risk Assessment

After the ISSP is reviewed, the initial risk assessment should be inspected to ensure that it identifies all apparent threats and vulnerabilities in the information system and is consistent with the guidance provided in the NNSA risk management methodology as described in NAP 14.1-C, *NNSA Baseline Cyber Security Program*. The risk assessment should also determine the overall level of risk present on the system given the type of data the system processes, the security controls on the system, and the system's operating environment. The risk assessment is completed before the system is fielded to verify that the security requirements specified during development have been met. Risk assessments shall be updated every time there is a change to the security controls on the system that might affect the residual risk to the system.

Step 6: Review the ISA

If this system will be connected to other information systems under the responsibility of another certifying or accrediting authority, the requirements for connectivity with the other system must be identified. The ISA is started during the Initiation Phase of the System Development Life Cycle (SDLC) and is refined during the Acquisition/Development Phase. However, the ISA may not be completed until the actual system Implementation Phase. Additional requirements on ISAs are contained in NAP 14.1-C, Chapter XXI.

Step 7: Negotiation

After steps 1 through 4 are complete, all the participants, including the program manager, the system owner, and CT will review the extent and scope of the planned C&A effort. The participants should review the security/system categorization for the system and ensure that it is appropriate. At this point, a schedule is set forth for the remaining steps in the C&A effort. After successful negotiation, the DAA approves the security plan.

The checklist in Figure III-1 on the following page provides a quick reference of all activities that should take place during Phase 1 of the C&A process.

Figure III-1. Phase 1 Checklist

Phase 1 Checklist	
	Has the scope of the C&A effort been defined?
	Has the security/system categorization been determined and documented?
	Have the Minimum Set of Security Controls been identified? Have any additional controls been identified? Has a review of the approved ISA been done? Has a PIA been conducted, if required?

	Has the Information System Security Plan been reviewed?
	Has the Risk Assessment been reviewed?
	Has the DAA approved the ISSP? Have any deviations (if applicable) been approved?

Phase 2: Verification

During the Verification phase, the ST&E team will conduct the testing to evaluate the effectiveness of the security controls on the information system, and then use the results of the ST&E to update the risk assessment and the ISSP, if necessary. The results of this phase will be documented in the final certification package. The certification package will then be presented to the DAA for a final accreditation decision.

Step 1: Conduct a Security Test and Evaluation (ST&E)

All controls identified in each ISSP are to be subjected to security control assessment procedure(s) during the C&A process to evaluate the status of control implementation with respect to security requirements and effectiveness.

- Under a “System”, “Site”, or “Type” form of accreditation, each control must be subjected to a ST&E process.

- Accreditation of additional instantiations (i.e., additional equivalent installations) may be based on a subset of the ST&E procedures used for the first instance. This subset, which is identified in the ST&E Procedures and approved by the DAA, must provide for overall assurance that future instantiations are equivalently implemented to the first instance.

- The ST&E procedure(s) used for the assessment/evaluation of a control for each additional instance must not be modified from those used to evaluate the first instance.

ST&E consists of three steps: creating the ST&E Plan, executing the test procedures, and documenting the results in the ST&E Report with recommended countermeasures.

Create the ST&E Plan

When developing the plan, testing objectives and ST&E procedure(s) shall be derived from the security controls identified in Phase 1. Each ST&E procedure, at a minimum, verifies that the security control is in effect and correctly implements the explicitly identified criteria in the control statement. ST&E procedure(s) must be developed for each control identified in the ISSP.

Each ST&E procedure must identify the specific control and associated assessment method(s) used to evaluate the control and support the determination of the security control effectiveness.

The following assessment methods will be used for the assessment of both unclassified and national security systems.

- Interview: Focused discussions with individuals or groups to facilitate understanding, achieve clarification, or obtain evidence.

- Examine: Checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence.

- Test: Exercising one or more assessment objects under specific conditions to compare actual with expected behavior.

Chapter VI, Security Category, describes the expected levels of assurances for the different impact levels (Low Baseline. Moderate Baseline, High Baseline) that must be used to guide the level of testing effort required for each impact level.

Execute the Test Plan

After the ST&E plan has been approved by the CA and the DAA, the test procedures in the plan shall be executed. An important part of the ST&E is a validated Contingency Plan and the careful review of security-related documentation, such as the risk assessment, PIA, ISSP, and the Contingency Plan in accordance with NNSA policy. Validation is achieved through (a) a table-top exercise, or exercising the plan and (b) documenting the results. These documents should be reviewed to ensure that they are 1) developed in accordance with the appropriate NNSA and Federal requirements, and 2) that they are up-to-date and usable for their intended purpose.

Expected Results

The expected results of the ST&E procedure must assure that all controls are specified, implemented, and operational consistent with the functional requirements of the control statement.

Create the ST&E Report and Recommend Countermeasures

After the testing activities are complete, the results from the testing should be documented in a ST&E report. The report should identify which controls are implemented effectively, which controls are implemented partially, and which controls are either not implemented, or are ineffective. These results will be used as input to update the risk assessment.

After the ST&E report is complete, the system owner and the program manager should discuss the appropriate countermeasures to be implemented. These countermeasures should address any security requirements that were found to be not implemented or ineffective. Countermeasures

may be implemented immediately or may be included as part of a remediation plan and schedule for an IATO, or the situation may be accepted by the DAA.

Step 2: Conduct a Risk Evaluation

This step involves using the results from the ST&E Report to determine the remaining risk for the system once corrective actions have been implemented to address results from the ST&E. Any necessary updates to the system's risk must be included in the form of an addendum to the system's original risk evaluation. Risk should be determined for both individual test results and the overall system or application. This risk determination will be included as part of the certification package.

Step 3: Update the ISSP and ISA

The ISSP will be updated to reflect any additional security controls or implementation changes as a result of the ST&E activities and the final risk assessment. Updates should also be made in the approved ISA and, if required, the PIA.

Step 4: Document Certification Findings

Once the certification activities are complete, the ST&E team will document the results from the certification process in a ST&E Report. This report will annotate the results and any relevant security issues identified during certification activities. These results will be compiled along with the other certification documents into a certification package and forwarded to the CA for review

Note: The ISSM and CA may be the same person. If they are not, then the certification package must be submitted to the ISSM by the CA. Figure III-2 shows the Verification Package contents.

Phase 2: Verification Package	
	Completed ST&E Report
	Approved ISSP including ISAs
	Completed PIA (if applicable)
	Completed SOR Notice if required
	Updated Risk Assessment

Figure III-2. Verification Package Contents

The CA will evaluate the risks and issues presented in the certification package. The CA then develops a Certification Statement that states the extent to which the system meets documented security requirements. As part of the Certification Statement, the CA also provides a recommendation for an accreditation decision The ISSM then submits the certification statement to the DAA.

Phase 3: Validation of Certification/Accreditation Decision

During the final step of Phase 3, the DAA will review the ST&E Report, weigh the residual risk, and decide whether to issue an accreditation or to deny accreditation. Based on an evaluation of residual risk, the ISSM's recommendation, the DAA will make a risk-based decision to grant system accreditation or to deny system accreditation because the risks to the system are not at an acceptable level. The accreditation decision will be documented in the final accreditation package, which consists of the accreditation letter and supporting documentation.

The following checklist in Figure III-3 provides a reminder of all the actions that should take place during Phase 3 of the C&A process.

Phase 3 Checklist	
	Has the ST&E Plan been created and approved?
	Has security testing been performed?
	Have Privacy Implications been reviewed (if required)?
	Has the approved ISA been reviewed?
	Has the ST&E Report been written?
	Has the Risk Evaluation been updated if required?
	If the ISSP has been updated, has the updated plan been approved by the DAA?
	Have the certification findings been documented?
	Has the certification package been forwarded to the ISSM?
	Has the ISSM reviewed the ST&E Report and forwarded it to the DAA?
	Has the DAA issued an accreditation decision? If so, has the DAA returned the C&A package to the ISSM?

Figure III-3. Phase 3 Checklist

Phase 4: Post-Accreditation Phase

During the post-accreditation phase, the system configuration will be managed to ensure that changes to the system are monitored, that they do not adversely affect the security posture of the system, and to facilitate follow-on C&A activities. Periodic testing (at least annually for critical infrastructure and key resources, and annually for all others) of the Contingency Plan and selected security controls is a necessary component of the Post-Accreditation Phase.

Configuration Management

Once the system or majo0r application has been officially accredited, the system owner must maintain configuration control over the system to ensure that the security posture of the system is not threatened by authorized or unauthorized changes to system software or hardware.

Security-relevant changes that are implemented are documented in the ISSP , design documentation (for software code changes), and/or the inventory list (for hardware and/or software changes). ***Security-significant changes (e.g., security-relevant software version changes, and operating system changes.), as determined by the DAA, will require re-accreditation activities to ensure that the system has not incurred additional risk.***

Configuration Management and Control

The purpose of this task is to define and document a baseline system configuration and document and assess proposed and actual changes to the information system. This task is composed of two sub-tasks.

- Documentation of the Information System Changes. The system owner ensures that proposed and actual changes to the system are documented , and compares these to the baseline configuration.

- Security Impact Analysis. The system owner ensures that each proposed or actual changes to the system are analyzed to determine the security impact.

4. SECURITY CONTROL MONITORING.

The purpose of this task is to detect unauthorized changes to the system configuration through monitoring and annual assessment of a selected set of controls. This task is completed via three sub-tasks.

- Security Control Selection. The ISSO ensures the selection of the technical, operational, assurance, and management security controls for monitoring and annual assessment. *The selection of controls must be approved by the DAA.*

- Selected Security Control Assessment. The ISSO ensures the assessment of any controls designated in the ISSP as needing monitoring and performance of self-assessments annually on the remaining controls.

- Status Reporting. The ISSO ensures that significant changes to the security posture of the information system are reported through the ISSM to the DAA.

Reaccreditation

Federal regulations mandate that systems be re-accredited every three (3) years or when security-significant changes are made to the system configuration. Program managers and system owners should keep this in mind when planning system changes. If the system is not significantly altered, the system owner should begin the C&A process for re-accreditation in a timely fashion to ensure that the process is complete before the three-year anniversary of the system accreditation has passed. The Figure III-4 on the following page shows the checklist of all the actions that should take place during Phase 4 of the C&A process.

Phase 4 Checklist	
	Has the system owner maintained configuration control?
	Have all security-relevant changes to the system been approved by the DAA ?
	Have the hardware and software inventories been updated every time the system configuration changed?
	If major system changes have been implemented, has the system been re-accredited in its new configuration?
	Is the three-year anniversary of the system accreditation approaching? If so, have plans for resources been made to begin the re-accreditation process?

Figure III-4. Phase 4 Checklist

APPENDIX A

ACCREDITATION LETTER SAMPLE

Security Accreditation Decision Letter (Authorization to Operate)

From: Authorizing Official Date:

To: ISSM

Subject: Security Accreditation Decision for [INFORMATION SYSTEM]

After reviewing the results of the security certification of the [INFORMATION SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] and the supporting evidence provided in the associated security accreditation package (including the current ISSP and the Security Testing and Evaluation report), I have determined that the risk to agency operations, agency assets, or individuals resulting from the operation of the information system is acceptable. Accordingly, I am issuing an *authorization to operate* the information system at the Control Baseline in its existing operating environment. The information system is accredited without any significant restrictions or limitations. This security accreditation is my formal declaration that adequate security controls have been implemented in the information system and that a satisfactory level of security is present in the system. The security accreditation of the information system will remain in effect as long as: (i) the required security status reports for the system are submitted to this office every [TIME PERIOD]; (ii) any vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk which is deemed unacceptable; and (iii) the system has not exceeded the maximum allowable time period between security accreditations in accordance with Federal or agency policy. A copy of this letter with all supporting security C&A documentation should be retained for the period of the system's accreditation.

Signature

Title

Enclosures

This page intentionally left blank.

APPENDIX B

SAMPLE SECURITY ACCREDITATION DECISION LETTER INTERIM AUTHORIZATION TO OPERATE (IATO)

Date:

From: Authorizing Official

To: ISSM

Subject: Security Accreditation Decision for [INFORMATION SYSTEM]

After reviewing the results of the security certification of the [INFORMATION SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] and the supporting evidence provided in the associated security accreditation package (including the current ISSP and the Security Test and Evaluation Report, I have determined that there is an overarching need to place the information system into operation or continue its operation due to mission necessity. Accordingly, I am issuing an *interim authorization to operate* the information system at the Control Baseline in its existing operating environment. An interim authorization is a limited authorization to operate the information system under specific terms and conditions for a limited period of time. The information system is *not* considered accredited during the period of limited authorization to operate. The terms and conditions of this limited authorization are described in Appendix A, Accreditation Letter Sample. A process must be established immediately to monitor the effectiveness of the security controls in the information system during the period of limited authorization. Monitoring activities should focus on the specific areas of concern identified during the security certification. Significant changes in the security state of the information system during the period of limited authorization should be reported immediately. This interim authorization to operate the information system is valid for [TIME PERIOD]. The limited authorization will remain in effect during that time period as long as: (i) the required security status reports for the system are submitted to this office every [TIME PERIOD]; (ii) any vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk which is deemed unacceptable; and (iii) continued progress is being made in the system's progress toward full accreditation. At the end of the period of limited authorization, the information system must be authorized to operate or the authorization for further operation will be denied. This office will monitor the schedule submitted with the request for interim approval during the period of limited authorization. A copy of this letter with all supporting security C&A documentation must be retained with the system documentation until the system has achieved final accreditation.

Signature

Title

Enclosures

This page intentionally left blank.

APPENDIX C

SAMPLE INTERCONNECTION SECURITY AGREEMENT

Purpose – The purpose of this ISA is to identify and document to all signatories satisfaction:

1. Existing risks and mitigation strategies for all of the systems being interconnected, regardless of whether they are General Support Systems (GSS) or Major Applications (MA). Note: Any automated process that relies on Information Technology (IT) must be considered either a GSS or a MA.

2. Any additional risks and mitigation strategies introduced through the interconnection of systems not under the operation control of the sponsoring agency.

3. Identification of systems participating in the interconnection,.

4. Appropriate levels of assurance to the satisfaction of all signatories that the documented risk and mitigation strategies are operating as stated and are effective.

5. Documentation of responsibilities and processes for mutual incident response and reporting; mutual management, maintenance, operation, and configuration management of the interface; and disconnection and re-connection of the systems.

INTERCONNECTION STATEMENT OF REQUIREMENTS – This section should contain:

A clear description of the systems covered by this agreement;

Each system's intended purpose and target community;

Data sensitivity (i.e., classification)

A description of the interconnection, including a graphic representation of the interconnection, the purpose of the interconnection, and a clear description of the authorities under which all of the systems operate. This includes statutory/regulatory requirements, project goals, and should also clearly state the responsible management units and system owners, and DAAs;

This agreement shall be reviewed on an annual basis and amended whenever a security-relevant change to the systems concerned are planned. A change log and a new signature page should be attached whenever these events occur.

SYSTEM SECURITY CONSIDERATIONS – General information, data descriptions and data/work flows should be documented in this section as well as risks and mitigation strategies

so that a clear picture is presented to each participant of any residual risk. To that end, the following documents shall be included (where data sensitivity allows) with the ISA:

Risk Assessments – A copy of the Risk Assessment for each system shall become an appendix to this agreement.

Security Test and Evaluation Plan/Report – Security Test and Evaluation Plans and subsequent reports for systems included in this agreement shall be amended by all participants to include the details of the agreement.

Security Assurance –Applicable Certification & Accreditation/Interim Authority to Operate

Executive Summaries/Sign-Off – An Executive summary shall be prepared that is tied directly to the portion of the ISA that contains all appropriate signatures. Conditions for revocation of an ISA authority shall appear in this area as well.

CHAPTER IV: NNSA MANAGEMENT, OPERATIONAL, AND TECHNICAL CONTROLS

This is the NNSA implementation of the DOE CIO TMR-1. The selection and specification of security controls for an information system is accomplished as part of a Department-wide information security program that involves the management of organizational risk—that is, the risk associated with the operation of an information system. The management of organizational risk is a key element in the Department's information security program and provides an effective framework for selecting the appropriate security controls for an information system—the security controls necessary to protect the operations and assets of the organization.

Managing organizational risk includes several important activities: (i) assessing risk; (ii) conducting cost-benefit analyses; (iii) selecting, implementing, and assessing security controls; and (iv) formally authorizing the information system for operation (also known as security accreditation). The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, Directives, Executive Orders, policies, standards, or regulations.

This NNSA NAP implements National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*; FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*; NIST Special Publication (SP) 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, and the DOE cyber security program criteria for the implementation of management, operational, and technical controls for information systems, DOE M 205.1-4.

This NAP defines NNSA requirements and recommended controls for information systems. The NNSA implementation of these security controls are based on the recommendations of the NIST SP 800-53, Revision 1 and the CNSS recommendations. The criteria are described by security control baseline (i.e., low, moderate, and high). Supplemental issue-specific NAPs provide more detail on some of the requirements and include processes for implementing the controls.

This NAP follows the NIST SP 800-53, Revision 1, structure utilizing the control Classes, Families, and Identifiers as shown in Table D-1. To uniquely identify each control, a numeric identifier is appended to the Family identifier to indicate that control within the Family. For example, PL-1 represents control number 1 within the Planning Family.

"SPECIAL" INFORMATION SYSTEMS. Extensive technical protection measures may be inappropriate and unnecessarily expensive for some information systems (e.g., single-user standalone systems, and legacy systems). The DAA will determine which of the management, operational and technical controls contained in this NAP are to be applied to those systems in the NNSA Elements.

PROTECTION REQUIREMENTS FOR SENSITIVE UNCLASSIFIED INFORMATION (SUI). A comprehensive listing of NNSA requirements for the protection of SUI, including Personally Identifiable Information (PII) is not possible within the context of this chapter. See Chapter VII for additional requirements for the protection of SUI. Table IV-1 provides a listing of all cyber classes, families, and identifiers.

Table IV-1. Cyber Security Control Classes, Families and Identifiers

Class	Family	Identifier
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessment	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

The requirements provide a unified and consistent approach to security controls to be addressed in the NNSA element's Cyber Security Program Plan (CSPP) and ISSPs.

An NNSA Element may specify and implement additional requirements in its CSPP to address specific risks, vulnerabilities, or threats within its operating unit.

REQUIREMENTS

Managing Organizational Risk

Each NNSA Element is to document its approach to managing organizational risk through the organization's CSPP. NNSA Element Managers are responsible for developing, documenting in the CSPP, and implementing policies and processes to develop an acceptable control baseline for each information system appropriate to the impact level of the system (see Chapter VI, Security Category). The CSPP will also describe the risk management or mission impact rationale for all criteria not fully addressed in the implementation policies.

The following activities related to managing organizational risk in the NNSA Element are paramount to an effective information security program and can be applied through the CSPP to both new and legacy information systems within the context of the System Development Life Cycle and the DOE Enterprise Architecture.

- Categorize information systems and the information resident within the system based on an impact analysis using Table 6 in Chapter III.

- Select an initial set of security controls (i.e., baseline) for the information system as a starting point for the risk assessment process, based on the FIPS 199 security categorization and the minimum security requirements defined in this document.

- Document the set of security controls ISSP for the information system including the NNSA Element's justification for any refinements or adjustments to the initial set of controls.

- Implement the security controls in the information system. For existing systems, some or all of the security controls selected may already be in place.

- Assess the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

- Authorize information system processing (or for legacy systems, authorize continued system processing) based upon a determination of the risk to organizational operations, organizational assets, or to individuals resulting from the operation of the information system and the decision that this risk is acceptable.

- Monitor and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis.

The following conventions are used in this Chapter**:**

- At the beginning of each Family section, a table is inserted which provides a summary of the controls required for that Family for each category of information system. Detailed information for each of the controls follows that table.

- Supplemental guidance is provided for the controls. In some cases, supplemental guidance is also provided for Control Enhancements. This information is provided for additional clarification of the intent of the control.

- Following each control's requirements statements is a table summarizing the controls required for Low, Moderate, or High information systems. Where there is one table, the controls apply to both classified and unclassified systems. Where there are two lines to the table, the controls noted on the shaded line apply to classified systems; the controls noted on the unshaded line apply to unclassified systems. (See control AC-10 for an example.)

FAMILY: ACCESS CONTROL CLASS: TECHNICAL

The cyber security roles defined in the NNSA PCSP are responsible for managing and coordinating access controls within the operating unit and ensuring implementation and compliance with the following Access Control policy for each information system in the NNSA Element.

Access Control Policy. Access control measures are designed to limit access to information system resources to authorized users, programs, processes, or other systems and to manage authorities and privileges granted to each user of the information system or application. These measures must include maintenance of 1) the association between a user identifier and an authenticator; 2) user authorizations and privileges; 3) user access to objects; 4) authority to grant access to objects and subjects; 5) authority to add, modify, and remove objects and subjects, 6) temporary and emergency accounts must be terminated within 24 hours, and 7) automatically disable inactive accounts within 3 months of the last use.

Access Controls				
Control Number	**Control Name**	**Protection Index**		
		Low	**Moderate**	**High**
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2 (1)(2)(3)(4)	AC-2 (1)(2)(3)(4)(5)	AC-2 (1)(2)(3)(4)(5)
AC-3	Access Enforcement	AC-3	AC-3 (1)(2)(3)	AC-3 (1)(2)(3)
AC-4	Information Flow Enforcement	AC-4	AC-4 (1)(2)	AC-4 (1) (2)
AC-5	Separation of Duties	AC-5	AC-5	AC-5
AC-6	Least Privilege	AC-6	AC-6 (1)	AC-6 (1)
AC-7	Unsuccessful Logon Attempts	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-9	Previous Logon Notification	Not required at this time. NNSA Elements may elect, at their discretion, to ensure that information systems notify the user, upon successful logon, of the last logon and the number of unsuccessful logon attempts since the last successful logon.		

Access Controls				
Control Number	**Control Name**	**Protection Index**		
		Low	**Moderate**	**High**
AC-10	Concurrent Session Control	Not required	AC-10	AC-10
			Not Required	AC-10 (1)
AC-11	Session Lock	AC-11	AC-11	AC-11
AC-12	Session Termination	AC-12	AC-12 (1)	AC-12 (1)
AC-13	Supervision and Review – Access Control	AC-13	AC-13 (1)	AC-13 (1)
AC-14	Permitted Actions without Identification and Authentication	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking	AC-15	AC-15	AC-15
		Not Required	AC-15	AC-15
AC-16	Automated Labeling	Not required at this time. NNSA Elements may elect, at their discretion, to ensure that information in storage, in process, or in transmission is appropriately labeled by an information system.		
AC-17	Remote Access	AC-17(1)	AC-17 (1)(2)(3)(4)(5)(6)	AC-17 (1)(2)(3)(4)(5)(6)(7)
AC-18	Wireless Access Restrictions	AC-18	AC-18 (1)(2)(3)(4)	AC-18 (1)(2)(3)(4)
AC-19	Access Control for Portable and Mobile Devices	AC-19	AC-19 (1)	AC-19 (1)
AC-20	Personally Owned Information Systems	AC-20	AC-20 (1)	AC-20 (1)
AC-21	Confidentiality of Data at Rest	AC-21	AC-21	AC-21
AC-22	Distinct Levels of Access	AC-22	AC-22	AC-22

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: NNSA Elements must develop, disseminate, and periodically review/update:

a. A formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Supplemental Guidance: The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required.

Control Enhancements: None.

LOW AC-1	**MOD** AC-1	**HIGH** AC-1

AC-2 ACCOUNT MANAGEMENT

Control: Manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The NNSA Element will:

a. Review information system accounts at least annually.

b. Identify authorized users of the information system and specify access rights/privileges.

c. Require proper identification for requests to establish information system accounts and approves all such requests.

d. Authorize and monitor the use of guest/anonymous accounts and remove, disable, or otherwise secures unnecessary account.

e. Notify account managers when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured.

f. Notify account managers when users' information system usage or need-to-know/need--to-share changes.

Supplemental Guidance: Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization should

consider the following aspects when granting access to the information and information systems: (i) A valid need-to-know/ need-to share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) Intended system usage.

Control Enhancements:

(1) The organization employs automated mechanisms to support the management of information system accounts.

(2) The information system automatically terminates temporary and emergency accounts after 24 hours.

(3) The information system automatically disables inactive accounts no later than 3 months after the last use.

(4) The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.

(5) The organization establishes and administers all privileged user accounts in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, Web administration).

LOW AC-2(1)(2)(3)(4)	**MOD** AC-2(1)(2)(3)(4)(5)	**HIGH** AC-2(1)(2)(3)(4)(5)

AC-3 ACCESS ENFORCEMENT

Control: Enforce assigned authorizations for controlling access to the system in accordance with applicable policy.

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant or NSA Type-1 Related security Control: SC13.

Control Enhancements:

(1) The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Enhancement Supplemental Guidance: Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

(2) The Mandatory Access Control (MAC), and/or Discretionary Access Control (DAC), and/or Role Based Access Control (RBAC) policies of the information system are implemented and configured to ensure only authorized users are able to perform security functions.

(3) The MAC, DAC, and/or RBAC policies of the information system and/or Operating System (OS) are implemented and configured to protect security relevant objects from unauthorized access, modification, and deletion. In the case of applications which enforce the security policy but are outside the protections of a trusted OS, the application must maintain the ability to protect itself.

LOW AC-3	**MOD** AC-3 (1)(2)(3)	**HIGH** AC-3 (1)(2)(3)

AC-4 INFORMATION FLOW ENFORCEMENT

Control: Enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems, as well as between shared components that transmit data at different levels, such as RD and NSI, in accordance with applicable policy.

Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Related security Control: SC7.

Control Enhancements:

(1) The information system implements information flow control enforcement using protected processing domains (e.g., domain type enforcement) as a basis for flow control decisions.

(2) The information system implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions. For further information on these policy mechanisms, refer to the Supplemental Guidance paragraphs for the control.

LOW AC-4	**MOD** AC-4 (1)(2)	**HIGH** AC-4 (1)(2)

AC-5 SEPARATION OF DUTIES

Control: Enforce separation of duties through assigned access privileges. The NNSA Element separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. Access control software resides on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion.

Supplemental Guidance: Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions. Through the use of access control software or site processes and procedures, users are prevented from having all of the necessary authority or information access to perform fraudulent activity without collusion.

Control Enhancements: None.

LOW AC-5	**MOD** AC-5	**HIGH** AC-5

AC-6 LEAST PRIVILEGE

Control: The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Supplemental Guidance: The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

Control Enhancement:

(1) The organization ensures that privileged accounts are created for users to perform privileged functions only; that is, privileged users use non-privileged accounts for all non--privileged functions.

Enhancement Supplemental Guidance: For example, SUDO for UNIX and Run As for a Windows system.

LOW AC-6 (1)	**MOD** AC-6 (1)	**HIGH** AC-6 (1)

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Control: Document in ISSPs and enforce a limit of no more than three consecutive invalid access attempts by a user during a two-hour time period. The information system must automatically lock the account/node for 15 minutes (or until authorized to be unlocked), or delays the next login prompt when the maximum number of unsuccessful attempts is exceeded. This control also applies to remote access logon attempts.

Supplemental Guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period.

Control Enhancements: None

LOW AC-7	**MOD** AC-7	**HIGH** AC-7

AC-8 SYSTEM USE NOTIFICATION

Control: Display an approved system-use notification message before granting system access informing potential users that:

a. The user is accessing a U.S. Government information system;

b. System usage may be monitored, recorded, and subject to audit;

c. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and

d. Use of the system indicates consent to monitoring and recording.

The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Supplemental Guidance: The following notice must be displayed:

*****WARNING**WARNING**WARNING**WARNING**WARNING*****

This is a Department of Energy (DOE) computer system. DOE computer systems are provided for the processing of official U.S. Government information only. All data contained within DOE computer systems is owned by the DOE, and may be audited, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on DOE computer systems to appropriate authorities.

USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS AUDITING, INTERCEPTION, RECORDING, READING, COPYING, CAPTURING, and DISCLOSURE OF COMPUTER ACTIVITY.

*****WARNING**WARNING**WARNING**WARNING**WARNING*****

Control Enhancements: None.

LOW AC-8	**MOD** AC-8	**HIGH** AC-8

AC-9 PREVIOUS LOGON NOTIFICATION

Control: If technically feasible, the information system notifies the user, upon successful logon, of the date and time of the last logon.

Supplemental Guidance: None

Control Enhancement:

(1) If technically feasible, the information system notifies the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.

LOW Not required	**MOD** Not required	**HIGH** Not required

AC-10 CONCURRENT SESSION CONTROL

Control: Limit the number of concurrent sessions for any user to one session.

Supplemental Guidance: Concurrent sessions are when a user accesses an information system once and invokes multiple sessions. Concurrent logons are when a user accesses an information system more than once from a logon/login perspective.

Control Enhancements:

(1) DAAs may make local determinations on the types of accounts (i.e., privileged) to which this applies.

LOW Not required	**MOD** AC-10	**HIGH** AC-10
LOW Not required	**MOD** Not required	**HIGH** AC-10(1)

AC-11 SESSION LOCK

Control: Prevent further access to the system by initiating a session lock after 10 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

Supplemental Guidance: Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the information system.

Control Enhancements: None

LOW AC-11	**MOD** AC-11	**HIGH** AC-11

AC-12 SESSION TERMINATION

Control: Automatically terminate a remote session after a period of inactivity specified in the system's ISSP.

Supplemental Guidance: A remote session is initiated whenever an organizational information system is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).

Control Enhancements:

(1) Automatic session termination applies to remote sessions.

LOW AC-12	**MOD** AC-12(1)	**HIGH** AC-12(1)

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

Control: Supervise and review the activities of users with respect to the enforcement and usage of information system access controls.

Supplemental Guidance: The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational policies. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities. The extent of the audit record reviews is based on the Trust Levels of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a Web proxy or e-mail servers and when specific circumstances warrant review of other audit records.

Control Enhancement:

(1) The organization employs automated mechanisms to facilitate the review of user activities.

LOW	AC-13	**MOD**	AC-13(1)	**HIGH**	AC-13(1)

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control: Identify and document specific user actions that can be performed on the information system without identification or authentication.

Supplemental Guidance: The organization allows limited user activity without identification and authentication for public Web sites or other publicly available information systems (e.g., individuals accessing a Federal information system at http://www.firstgov.gov). Related security Control: IA2.

Control Enhancement:

(1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives (e.g., a weapons system).

LOW	AC-14	**MOD**	AC-14 (1)	**HIGH**	AC-14 (1)

AC-15 MARKING

Control: Mark output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

Supplemental Guidance: The user or the system marks all output from the system (classified data and data requiring special handling) to reflect the classification and sensitivity of the data (e.g., classification level, classification category, and handling caveats). Markings shall be retained with the data. Markings will be in accordance with DOE M 470.4-4.

Control Enhancements: None

LOW	AC-15	**MOD**	AC-15	**HIGH**	AC-15
LOW	Not required	**MOD**	AC-15	**HIGH**	AC-15

AC-16 AUTOMATED LABELING

Control: The information system appropriately labels information in storage, in process, and in transmission. Information labeling is accomplished in accordance with:

a. Access control requirements;

b. Special dissemination, handling, or distribution instructions; or

c. As otherwise required to enforce information system security policy.

Supplemental Guidance: Automated labeling refers to labels employed on internal data structures (e.g., records, files) within the information system.

Control Enhancements:

(1) Data released by a producer shall either be explicitly or implicitly labeled. If the data is of a different classification or sensitivity than the source (e.g., session window) from which it was extracted, then the producer shall take some explicit action to associate the correct label with the data.

(2) Implicit labels are generally based on the classification and sensitivity level of the communications session over which the data is sent, and are employed when the value of explicit labels associated with the data cannot be trusted.

LOW Not required	**MOD** Not required	**HIGH** Not required

AC-17 REMOTE ACCESS

Control: Document, monitor, and control all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.

Supplemental Guidance: Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public Web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source or request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology).

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. Policies and procedures of the user control group must be followed.

(2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.

(3) The organization controls all remote accesses through a limited number of managed access control points.

(4) The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

(5) The information system restricts all remote access sessions by privileged users to those with strong authentication. Related to IA2.

Enhancement Supplemental Guidance: Strong authentication is defined as the information system employs a multifactor authentication process and/or device to generate a onetime password that is highly resistant to replay attacks.

(6) The organization ensures that users protect information about the remote access mechanisms from unauthorized use and disclosure.

(7) The organization ensures that remote sessions for privileged user functions employ additional security measures and that each remote session is comprehensively audited.

Enhancement Supplemental Guidance: Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell (SSH), or Virtual Private Networking with blocking mode enabled.

LOW AC-17 (1)	**MOD** AC-17 (1)(2)(3)(4)(5)(6)	**HIGH** AC-17 (1)(2)(3)(4)(5)(6)(7)

AC-18 WIRELESS ACCESS RESTRICTIONS

Control: Establish usage restrictions and implementation guidance for wireless technologies and document, monitor, and control wireless access to the information system.

Supplemental Guidance: None

Control Enhancements:

(1) The organization uses authentication and encryption to protect wireless access to the information system.

Enhancement Supplemental Guidance: The appropriate level of encryption strength will be selected based on the classification and/or sensitivity of the data.

(2) The organization scans for unauthorized wireless access points quarterly and takes appropriate action if such an access point is discovered.

(3) The organization ensures that wireless computing and networking capabilities within all IT resources are implemented in accordance with organizational wireless policies and technical guidelines.

(4) Wireless computing capabilities are not independently configured by end users, except through the use of approved scripts. Unused wireless computing and networking capabilities internally embedded in interconnected IT assets are normally disabled by changing factory defaults, settings or configurations prior to issue to end users.

LOW AC-18	**MOD** AC-18 (1)(2)(3)(4)	**HIGH** AC-18 (1)(2)(3)(4)

AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES

Control: Establish usage restrictions and implementation guidance for portable and mobile devices and document, monitor, and control device access to organizational information systems.

Supplemental Guidance: Portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are only allowed access to organizational information systems in accordance with organizational security policies and procedures. Security policies and procedures include device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), configuration management, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Related security controls: MP4 and MP5.

Control Enhancement:

(1) Employ removable hard drives or cryptography to protect information on portable and mobile devices.

LOW AC-19	**MOD** AC-19(1)	**HIGH** AC-19(1)

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

Control: Restrict the use of external information systems or components for official U.S. Government business involving the processing, storage, or transmission of Federal information.

Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g.,

computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by non-Federal Governmental organizations; and Federal information systems that are not owned by, operated by, or under the direct control of the organization.

Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational information systems and information that are intended for public access (e.g., individuals accessing Federal information through public interfaces to organizational information systems). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum trust level and security impact category of information that can be processed, stored, and transmitted on the external information system.

Control Enhancement:

(1) Prohibit authorized individuals from using an external information system to access the Element's information system or to process, store, or transmit organization controlled information except in situations where the organization:

(a) Can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan; or

(b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system; or

(c) The Element's system being accessed has protections in place to mitigate deficiencies on the connecting system.

LOW AC-20	**MOD** AC-20 (1)	**HIGH** AC-20 (1)

AC-21 CONFIDENTIALITY OF DATA AT REST

Control: Encrypt data at rest if required by the information owner or Departmental policy.

Supplemental Guidance: None

Control Enhancements: None

LOW AC-21	**MOD** AC-21	**HIGH** AC-21

AC-22 DISTINCT LEVELS OF ACCESS

Control: Provide at least three distinct levels of access, regardless of user interface, to all internal classified, sensitive, and unclassified information.

a. Open access to general information that is accessible to all authorized users with network access. Access does not require an audit transaction.

b. Controlled access to information that is accessible to all authorized users upon the presentation of an individual authenticator. Access is recorded in an audit transaction.

c. Restricted access to need-to-know information that is accessible only to an authorized community. Authorized users must present an individual authenticator and have either a demonstrated or validated need-to-know. All access to need-to-know information and all failed access attempts are recorded in audit transactions.

Supplemental Guidance: None

Control Enhancements: None.

LOW AC-22	**MOD** AC-22	**HIGH** AC-22

FAMILY: AWARENESS AND TRAINING CLASS: OPERATIONAL

Cyber security awareness consists of reminders that focus the user's attention on the concept of cyber security in the user's daily routine. Awareness provides a general cognizance or mindfulness of one's actions, and the consequences of those actions. Cyber security training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge, producing relevant and necessary security skills and competencies in those who access or manage NNSA information and resources.

Training Policy. Once granted legitimate access, authenticated users are expected to use information system resources and information only in accordance with the organizational security policy. In order for this to be possible, these users must be adequately trained both to understand the purpose and need for security controls and to be able to make secure decisions with respect to their discretionary actions. Authenticated users of the system must be adequately trained, enabling them to (1) effectively implement organizational security policies with respect to their discretionary actions and (2) support the need for non-discretionary controls implemented to enforce these policies prior to being granted access to information.

Awareness and Training				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1
AT-2	Security Awareness	AT-2	AT-2	AT-2
AT-3	Security Training	AT-3	AT-3	AT-3
AT-4	Security Training Records	AT-4	AT-4	AT-4
AT-5	Contact with Security Groups and Associations	Not required at this time.		

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: Develop, document, disseminate, and periodically review and/or update:

a. A formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

Supplemental Guidance: The security awareness and training policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required.

Control Enhancements: None.

LOW AT-1	**MOD** AT-1	**HIGH** AT-1

AT-2 SECURITY AWARENESS

Control: Provide security awareness training within 30 days to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and at least annually thereafter. This instruction must present a core

set of generic cyber security terms and concepts for all personnel (Federal employees and contractors) as a baseline for role=based learning, expands on those basic concepts, and provides a mechanism for students to relate and apply the information learned on the job.

Supplemental Guidance: The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access.

Control Enhancements: None.

LOW AT-2	**MOD** AT-2	**HIGH** AT-2

AT-3 SECURITY TRAINING

Control: Identify personnel with significant information cyber security roles and responsibilities, document those roles and responsibilities, and provides appropriate cyber security training before authorizing access to the system. Establish and, at least bi-annually (every two years), execute training plans for these personnel covering the training topics described in NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model.*

Supplemental Guidance: The organization determines the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides system managers, system and network administrators, and other personnel having access to system-level software, adequate technical training to perform their assigned duties.

Control Enhancements: None.

LOW AT-3	**MOD** AT-3	**HIGH** AT-3

AT-4 SECURITY TRAINING RECORDS

Control: Document and monitor individual information system security training activities including basic security awareness training and specific information system security training.

Supplemental Guidance: None

Control Enhancements: None.

LOW AT-4	**MOD** AT-4	**HIGH** AT-4

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

Control: Establish and maintain contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security related information including threats, vulnerabilities, and incidents.

Supplemental Guidance: To facilitate ongoing security education and training for organizational personnel in an environment of rapid technology changes and dynamic threats, the organization establishes and institutionalizes contacts with selected groups and associations within the security community. The groups and associations selected are in keeping with the organization's mission requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Control Enhancements: None.

LOW Not required	**MOD** Not required	**HIGH** Not required

FAMILY: AUDIT AND ACCOUNTABILITY CLASS: TECHNICAL

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can support individual accountability, a means to reconstruct events, detect intrusions, and identify problems. System audit trails, or event logs, provide a record of events in support of activities to monitor and enforce the information system security policy.

Audit and Accountability				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
AU-1	Audit and Accountability	AU-1	AU-1	AU-1

Audit and Accountability				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
	Policy and Procedures			
AU-2	Auditable Events	AU-2	AU-2	AU-2 (1)(2)
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5(1)	AU-5 (1)(2)
AU-6	Audit Monitoring, Analysis, and Reporting	AU-6	AU-6 (1)	AU-6 (1)(2)(3)
AU-7	Audit Reduction and Report Generation	AU-7	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	AU-8	AU-8	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9 (1)	AU-9 (1)
AU-10	Non-repudiation	AU-10	AU-10	AU-10
AU-11	Audit Retention	AU-11	AU-11(1)	AU-11(1)
AU-12	Session Audit	Not required. (See information at AU-12.)		

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control: Document, disseminate, and periodically review and/or update:

a. A formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Supplemental Guidance: The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required.

Control Enhancements: None

LOW AU-1	**MOD** AU-1	**HIGH** AU-1

AU-2 AUDITABLE EVENTS

Control:

As a minimum, the following auditable events must be captured:

- Start-up and shutdown of the audit functions;
- Successful use of the user security attribute administration functions
- All attempted uses of the user security attribute administration functions
- Identification of which user security attributes have been modified
- Successful and unsuccessful logons and logoffs
- Unsuccessful access to security relevant files including creating, opening, closing, modifying, and deleting those files
- Changes in user authenticators
- Blocking or blacklisting user IDs, terminals, or access ports
- Denial of access for excessive logon attempts
- System access by privileged users (privileged activities at the system (either physical or logical consoles) and other system-level access by privileged users). Users will not have administrative privileges to local systems, unless the systems are standalone.
- Starting and ending times for each access to the system.

  Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. Audit records can be generated at various levels of abstraction, including at the packet level as information traverse the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions.

Control Enhancements:

(1) The information system provides the capability to compile audit records from multiple components throughout the system into a system wide (logical or physical), time correlated audit trail.

(2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.

(3) The organization periodically reviews and updates the list of organization-defined auditable events.

LOW AU-2	**MOD** AU-2	**HIGH** AU-2 (1) (2)

AU-3 CONTENT OF AUDIT RECORDS

Control: Capture sufficient information in audit records to establish date and time of the event, what events occurred, the sources of the events, and the outcomes of the events.

Supplemental Guidance: Examples of audit record content includes: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user and/or subject identity; and (v) the outcome (success or failure) of the event. Auditable events are defined under AU2.

Control Enhancements:

(1) The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

(2) The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.

LOW AU-3	**MOD** AU-3 (1)	**HIGH** AU-3 (1) (2)

AU-4 AUDIT STORAGE CAPACITY

Control: Allocate sufficient audit record storage capacity and configure auditing to prevent such capacity being exceeded. Records that exceed the storage capacilty can be backed up to a different file.

Supplemental Guidance: The organization provides sufficient audit storage capacity, taking into account the auditing to be performed and the online audit processing requirements. Related security controls: AU2, AU5, AU6, AU7 and SI4.

Control Enhancements: None.

LOW AU-4	**MOD** AU-4	**HIGH** AU-4

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: In the event of an audit failure or 80% of audit storage capacity being reach, alert appropriate organization officials and take the additional actions specified by the system's ISSP; e.g., shut down the system, overwrite oldest audit records, stop generating audit records.

Supplemental Guidance: Audit processing failures include, for example, software and/or hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related security Control: AU4.

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment:* ***the percentage of maximum audit record storage capacity, as specified in the information system SSP***].

(2) The information system provides a real-time alert when the audit failure events occur: [*Assignment:* ***audit failure events requiring real-time alerts, as specified in the information system SSP***].

LOW AU-5	**MOD** AU-5(1)	**HIGH** AU-5 (1) (2)

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: Regularly review and/or analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization reviews the audit records at least on a weekly basis and reports findings to appropriate officials, and takes necessary actions.

(2) The organization employs automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications.

(3) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(4) The information system provides the ability for an administrator to set alert thresholds for all auditable events.

Enhancement Supplemental Guidance: Alert thresholds should be measured in terms of a utilization level maintained for a defined time period. Short spikes in the system health metrics should not normally be cause for alarm, rather abnormal levels over time should be cause for alarm.

(5) The information system enforces configurable thresholds to determine whether or not all network traffic can be handled and controlled. If a threshold has been met, the system shall process existing traffic until the threshold has been reduced before accepting new traffic for processing.

LOW AU-6	**MOD** AU-6 (1)	**HIGH** AU-6 (1) (2) (3) (4) (5)

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Control: Provide an audit reduction and report generation capability for each information system.

Note that it may not be possible to perform reduction of audit logs on all machines, especially on embedded systems.

Supplemental Guidance: Audit reduction, review, and reporting tools support after the fact investigations of security incidents without altering original audit records.

Control Enhancements:

(1) The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.

LOW AU-7	**MOD** AU-7 (1)	**HIGH** AU-7 (1)

AU-8 TIME STAMPS

Control: Provide time stamps for use in audit record generation.

Supplemental Guidance: Time stamps (including date and time) of audit records are generated using internal system clocks.

Control Enhancements:

(1) The organization synchronizes internal information system clocks quarterly.

LOW AU-8	**MOD** AU-8	**HIGH** AU-8 (1)

AU-9 PROTECTION OF AUDIT INFORMATION

Control: Protect system audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Control Enhancement:

(1) The information system will back up the audit records not less than weekly onto a different system or media than the system being audited.

LOW AU-9	**MOD** AU-9 (1)	**HIGH** AU-9 (1)

AU-10 NONREPUDIATION

Control: The information system provides the capability to determine whether a given individual took a particular action.

Supplemental Guidance: Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Nonrepudiation protects against later false claims by an individual of not having taken a specific action. Nonrepudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Nonrepudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an e-mail, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts, time stamps).

Control Enhancements:

(1) The information system associates the identity of the data producer with the data itself.

Enhancement Supplemental Guidance: Supports audit requirements that allow appropriate authorities the means to identify who produced the data.

(2) The information system validates the binding of the producer's identity to the data.

Enhancement Supplemental Guidance: This mitigates the risk that data is modified between production and review. A typical approach is validation of a cryptographic checksum.

(3) The information system will maintain reviewer and/or releaser identity and credentials within the chain of custody, as well as the integrity of data labels and markings for all information that is reviewed and/or released.

Enhancement Supplemental Guidance: If the reviewer is a human or if the review function is automated but separate from the release and/or transfer function, then the information system associates the identity of the reviewer of the data to be released with the data itself and the data's label and marking. In the case of a human reviewer, this requirement provides appropriate authorities the means to identify who reviewed and released the data, and in the case of automated reviewers, this helps ensure that only the approved review function was employed.

(4) The information system validates the binding of the reviewer's identity to the data and label and marking at the transfer and/or release point prior to release and/or transfer to another domain.

Enhancement Supplemental Guidance: This mitigates the risk that data is modified between review and transfer and/or release.

LOW AU-10	**MOD** AU-10	**HIGH** AU-10

AU-11 AUDIT RECORD RETENTION

Control: Retain audit records for the time period specified in the system's ISSP and as consistent with Departmental and National Archives and Records Administration retention periods, to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance: The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. Audit retention time period will be in accordance with Federal Laws, Statutes, and national policy.

Control Enhancements:

(1) The organization retains audit records for at least 6 months.

LOW AU-11	**MOD** AU-11 (1)	**HIGH** AU-11 (1)

AU-12 SESSION AUDIT

Control: The information system has the ability to remotely view, listen to, log, and capture all content related to a specific user in real time.

Supplemental Guidance: There are legal issues related to this ability, and thus it should be developed, integrated, and used under the guidance of legal counsel.

Control Enhancements:

(1) The information system provides the ability to capture the entire session data associated with a user in real-time.

(2) The information system has the ability to initiate the audit processes at system startup.

LOW Not required	**MOD** Not required	**HIGH** Not required

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS CLASS: MANAGEMENT

C&A is the process of formal assessment, testing (certification), and acceptance (accreditation) of system security controls that protect information systems and data stored in and processed by those systems. It is a process that encompasses the system's life cycle and ensures that the risk of operating a system is recognized, evaluated, and accepted. The C&A process implements the concept of "adequate security," or security commensurate with risk, including the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

Certification, Accreditation, and Security Assessment				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**

Certification, Accreditation, and Security Assessment				
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	CA-1	CA-1	CA-1
CA-2	Security Assessments	CA-2	CA-2	CA-2
CA-3	Information System Connections	CA-3	CA-3	CA-3
CA-4	Security Certification	CA-4(1)	CA-4(1)	CA-4 (1)
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5
CA-6	Security Accreditation	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7 (1)	CA-7 (1)(2)

CA-1 CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICIES AND PROCEDURES

Control: Develop, disseminate, and periodically review and/or update:

a. Formal, documented, security assessment and C&A policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the security assessment and C&A policies and associated assessment, certification, and accreditation controls.

Supplemental Guidance: The security assessment and C&A policies and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The organization, in concert with the DAA, defines what constitutes a significant change to the information system to achieve consistent security reaccreditations.

Control Enhancements: None.

LOW CA-1	**MOD** CA-1	**HIGH** CA-1

CA-2 SECURITY ASSESSMENTS

Control: Conduct an assessment of the security controls in the information system at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Supplemental Guidance: This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems and applications be assessed with a frequency depending on risk, but no less than annually. To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) security certifications conducted as part of an information system accreditation or reaccreditation process (see CA4); (ii) continuous monitoring activities (see CA7); or (iii) testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness).

Related security controls: CA4, CA6, CA7 and SA11.

Control Enhancements: None.

LOW CA-2	**MOD** CA-2	**HIGH** CA-2

CA-3 INFORMATION SYSTEM INTERCONNECTIONS

Control: Explicitly authorize all interconnections between information systems, as well as between shared components that transmit data at different levels, such as RD and NSI, from different certification or accreditation boundaries through the use of system connection agreements (where applicable) and monitor and/or control the system interconnections on an ongoing basis.

Supplemental Guidance: Since security categorizations apply to individual information systems, as well as the enterprise NNSA Elements should carefully consider the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks. Related security controls: SC7 and SA9.

Control Enhancements: None.

LOW CA-3	**MOD** CA-3	**HIGH** CA-3

CA-4 SECURITY CERTIFICATION

Control: Perform an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Supplemental Guidance: A security certification is conducted by the organization in support of the requirement for accrediting the information system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring (see CA7). The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment.

Control Enhancement:

(1) Employ a certification agent or certification team to conduct an assessment of the security controls in the information system.

Enhancement Supplemental Guidance: A certification agent or certification team is any individual or group capable of conducting an impartial assessment of an organizational information system.

LOW CA-4 (1)	**MOD** CA-4 (1)	**HIGH** CA-4 (1)

CA-5 PLAN OF ACTION AND MILESTONES

Control: Based on DAA determination, develop a plan of action and milestones (POA&M) for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies and to reduce or eliminate known vulnerabilities in the system. The POA&M must be updated quarterly.

Supplemental Guidance: If the DAA considers it necessary, the plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones.

Control Enhancements: None.

LOW CA-5	**MOD** CA-5	**HIGH** CA-5

CA-6 SECURITY ACCREDITATION

Control: Authorize (i.e., accredit) the information system for processing before operations and update the authorization at least every three years or when there is a significant change to the system.

Supplemental Guidance: Security assessments conducted in support of security accreditations are called security certifications. The security accreditation of an information system is not a static process. Related security controls: CA2, CA4 and CA7.

Control Enhancements: None.

LOW CA-6	**MOD** CA-6	**HIGH** CA-6

CA-7 CONTINUOUS MONITORING

Control: Continuously monitor the effectiveness and adequacy of security controls in the information system.. As a minimum, those security controls that are volatile or critical to protecting the information system are assessed at least annually. Testing of critical infrastructure and key resources must be accomplished annually; bi-annual testing must be accomplished for all other resources.

Supplemental Guidance: The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with national policy, the organization assesses a subset of the controls annually during continuous monitoring. The selection of an appropriate subset of security controls is based on: (i) the security categorization of the information system and risk to the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or grounds for confidence) that the organization must have in determining the effectiveness of the security controls in the information system.

The organization can use the current year's assessment results obtained during continuous monitoring to meet the annual FISMA assessment requirement (see CA2). This control is closely related to and mutually supportive of the activities required in monitoring configuration changes to the information system. A rigorous and well executed continuous monitoring process significantly reduces the level of effort required for the reaccreditation of the information system. Related security controls: CA2, CA4, CA5, CA6 and CM4.

Control Enhancements:

(1) The organization employs a certification agent or certification team to monitor the security controls in the information system on an ongoing basis.

(2) The organization will plan, schedule, and conduct performance testing that includes periodic, unannounced in-depth monitoring and specific penetration testing to ensure compliance with all vulnerability mitigation procedures.

LOW CA-7	**MOD** CA-7 (1)	**HIGH** CA-7 (1)(2)

FAMILY: CONFIGURATION MANAGEMENT CLASS: OPERATIONAL

Configuration Management. Measures to ensure the protection features specified in 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. A configuration management process must be implemented to detect any changes in system hardware, software, and firmware components that will modify or deviate from the approved minimum information system security configuration standard or the level of risk accepted by the DAA.

Configuration Management				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1)	CM-2 (1) (2)
CM-3	Configuration Change Control	CM-3	CM-3 (2)(3)	CM-3 (1)(2)(3)
CM-4	Monitoring Configuration Changes	CM-4	CM-4	CM-4
CM-5	Access Restrictions for Change	CM-5	CM-5 (1)(2)(4)	CM-5 (1)(2)(3)
CM-6	Configuration Settings	CM-6	CM-6 (2)	CM-6 (1)(2)
CM-7	Least Functionality	CM-7	CM-7 (1)(2)	CM-7 (1)(2)
CM-8	Information System Component Inventory	CM-8	CM-8 (1)	CM-8 (1)(2)

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control: Develop, disseminate, and periodically review and/or update:

a. A formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, compliance and the establishment of an entity to enforce the policy (i.e., Configuration Control Board); and

b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Supplemental Guidance: The configuration management policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required.

Control Enhancements: None.

LOW CM-1	**MOD** CM-1	**HIGH** CM-1

CM-2 BASELINE CONFIGURATION

Control: Develops, document, and maintain a current baseline configuration of the information system and an inventory of the system's constituent components.

Supplemental Guidance: This control establishes a baseline configuration for the information system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. The baseline configuration also provides the organization with a well defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs and/or objectives. Related security controls: CM6, CM8.

Control Enhancements:

(1) The organization updates the baseline configuration of the information system as an integral part of information system component installations.

(2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

LOW CM-2	**MOD** CM-2 (1)	**HIGH** CM-2 (1)(2)

CM-3 CONFIGURATION CHANGE CONTROL

Control: Document and control configuration changes to the information system. The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the information system include successful results from the security analysis of the change. The organization audits activities associated with configuration changes to the information system.

Supplemental Guidance: Configuration change control involves the systematic proposal, justification, implementation, test and/or evaluation, review, and disposition of changes to the information system, including upgrades and modifications. Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers). Related security controls: CM4, CM6, and SI2.

Control Enhancements:

(1) The organization employs automated mechanisms to:

(a) Document proposed changes to the information system;

(b) Notify appropriate approval authorities;

(c) Highlight approvals that have not been received in a timely manner;

(d) Inhibit change until necessary approvals are received; and

(e) Document completed changes to the information system.

(2) The organization establishes a CM control board, which includes the Information System Security Manager (ISSM), or Information System Security Officer (ISSO) as a member(s).

(3) All National Security Systems (NSS) are under the control of a chartered configuration control board (CCB) that meets regularly. The CCB reviews and approves all proposed information system changes, to include interconnections to other information systems.

LOW CM-3	**MOD** CM-3 (2)(3)	**HIGH** CM-3 (1)(2)(3)

CM-4 MONITORING CONFIGURATION CHANGES

Control: Monitor changes to the information system by conducting security impact analyses to determine the effects of the changes. After the information system is changed (including

upgrades and modifications), the organization checks the security features to verify that the features are still functioning properly. The organization audits activities associated with configuration changes to the information system.

Supplemental Guidance: Prior to change implementation, and as part of the change approval process, the Information System Security Manager (ISSM), or Information System Security Officer (ISSO) analyzes changes to the information system for potential security impacts. Monitoring configuration changes and conducting security impact analyses are important elements with regard to the ongoing assessment of security controls in the information system. Related security Control: CA7.

Control Enhancements: None.

LOW CM-4	**MOD** CM-4	**HIGH** CM-4

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control: Approve individual access privileges and enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes.

Supplemental Guidance: Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals obtain access to information system components for purposes of initiating changes, including upgrades, and modifications.

Control Enhancements:

(1) The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

(2) The organization limits and periodically reviews system developer privileges to change code and system data directly within a production environment.

(3) The organization limits system developer privileges to change code and system data directly within a production environment and reevaluates them on a 90 day cycle.

(4) System libraries are managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.

LOW CM-5	**MOD** CM-5(1)(2)(4)	**HIGH** C M-5 (1)(2)(3)(4)

CM-6 CONFIGURATION SETTINGS

Control:

a. Establish mandatory configuration settings for information technology products employed within the information system, where possible. See the Supplemental Guidance.

b. Configure the security settings of information technology products to the most restrictive mode consistent with operational requirements;

c. Document the configuration settings; and

d. Enforce the configuration settings in all components of the information system.

Supplemental Guidance: Configuration settings are the configurable parameters of the information assurance products that comprise the information system. Organizations monitor and control changes to the configuration settings in accordance with organizational policies and procedures. FISMA reporting instructions provide guidance on configuration requirements for Federal information systems. Related security controls: CM2, CM3, and SI4.

Control Enhancements:

(1) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.

(2) The information system and any modifications to the system baseline must demonstrate conformance to security configuration technical implementation guides prior to being introduced into a production environment.

LOW CM-6	**MOD** CM-6 (2)	**HIGH** CM-6 (1)(2)

CM-7 LEAST FUNCTIONALITY

Control: Configure the information system to provide only essential capabilities and document in the system's ISSP specific prohibitions and/or restrictions upon the use of functions, ports, protocols, and/or services. The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services* ***documented in the information system SSP***].

Supplemental Guidance: Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions).

Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. The functions and services provided by information systems, or individual components of information are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing systems).

Control Enhancements:

(1) The organization reviews the information system at least annually to identify and eliminate unnecessary functions, ports, protocols, and/or services.

(2) The information system complies with ports, protocols, and services guidance and organizational registration requirements.

LOW	CM-7	**MOD**	CM-7 (1)(2)	**HIGH**	CM-7 (1)(2)

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Control: Develop, document, and maintain a current inventory of the components of the information system and relevant ownership information.

Supplemental Guidance: The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system and/or component owner). The component inventory is consistent with the accreditation boundary of the information system. Related security controls: CM2 and CM6.

Control Enhancements:

(1) The organization updates the inventory of information system components as an integral part of component installations.

(2) The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

LOW	CM-8	**MOD**	CM-8 (1)	**HIGH**	CM-8 (1)(2)

FAMILY: CONTINGENCY PLANNING AND DISASTER RECOVERY CLASS: OPERATIONAL

Contingency Planning details the necessary procedures required to protect the continuing performance of core business functions and services, including information and information system services, during an outage.

Contingency Planning				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1 (1)	CP-1 (1)
CP-2	Contingency Plan	CP-2*	CP-2 (1)(2)*	CP-2 (1)(2)(3)*
CP-3	Contingency Training	CP-3	CP-3 (1)	CP-3 (1)(2)
CP-4	Contingency Plan Testing	CP-4	CP-4(1)	CP-4 (1)*
CP-5	Contingency Plan Update	CP-5	CP-5	CP-5
CP-6	Alternate Storage Sites	Not Required	CP-6 (1)(3)	CP-6 (1)(2)(3)(4)(5)
CP-7	Alternate Processing Site	Not Required	CP-7 (1)(2)(3)	CP-7 (1)(2)(3)(4)(5)
CP-8	Telecommunications Services	Not Required	CP-8 (1)(2)	CP-8 (1)(2)(3)(4)
CP-9	Information System Backup	CP-9	CP-9 (1)(4)	CP-9 (1)(2)(3)(4)
CP-10	Information System Recovery and Reconstitution	CP-10 (2)	CP-10 (1)(2)	CP-10 (1)(2)(3)

CP-1 CONTINGENCY PLANNING AND DISASTER RECOVERY POLICY AND PROCEDURES

Control: Develop, disseminate, and periodically review and update:

a. A formal, documented, contingency and disaster recovery planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the contingency and disaster recovery planning policy and associated contingency planning controls.

Supplemental Guidance: The contingency and disaster recovery planning policy and procedures are consistent with applicable Federal laws, directives, policies, regulations, standards, and guidance. The contingency and disaster recovery planning policy can be

included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required.

Control Enhancement:

(1) The organization develops and implements procedures to assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security related system software.

LOW CP-1	**MOD** CP-1 (1)	**HIGH** CP-1 (1)

CP-2 CONTINGENCY AND DISASTER RECOVERY PLAN

Control: Develop and implement a contingency plan and disaster recovery plan for each information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

Supplemental Guidance: None

Control Enhancements:

(1) The organization coordinates contingency plan development with organizational elements responsible for related plans.

Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.

(2) The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.

(3) The organization explicitly identifies mission and business essential functions and establishes associated restoration priorities and metrics. These activities must be linked to the BIA process.

* For systems with a level of concern for **availability** of HIGH:

(4) The organization plans and provides sufficient capacity to support partial restoration of mission or business essential functions.

(5) The organization plans and provides for the smooth transfer of all mission or business essential functions to alternate processing or facilities with little or no loss of operational continuity. Continuity is sustained through restoration to primary processing or facilities.

LOW CP-2*	**MOD** CP-2 (1)(2)*	**HIGH** CP-2(1)(2)(3)*

CP-3 CONTINGENCY AND DISASTER RECOVERY TRAINING

Control: Train personnel in their contingency and disaster recovery roles and responsibilities with respect to the information system and provide refresher training at least annually.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization incorporates simulated events into contingency and disaster recovery training to facilitate effective response by personnel in crisis situations.

(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

LOW CP-3	**MOD** CP-3 (1)	**HIGH** CP-3 (1)(2)

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

Control: The organization:

a. Test and/or exercise the contingency and disaster recovery plans for the information system at least annually using organization—defined tests and/or exercises to determine the plans' effectiveness and the organization's readiness to execute the plan; and

b. Review the contingency plan test and exercise results, and initiate corrective actions.

Supplemental Guidance: There are several methods for testing and/or exercising contingency and disaster recovery plans to identify potential weaknesses (e.g., full-scale testing, functional and/or tabletop exercises). Testing and/or exercises also include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to operations in accordance with the plan.

Control Enhancements:

(1) The organization coordinates contingency and disaster recovery plan testing and/or exercises with organizational elements responsible for related plans.

Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.

* For systems with a level of concern for **availability** of HIGH:

(2) The organization tests and/or exercises the contingency and disaster recovery plans at the alternate processing site to familiarize personnel with the facility and available resources and to evaluate the site's capabilities to support operations.

(3) It is recommended that the organization employ automated mechanisms to more thoroughly and effectively test and/or exercise the contingency and disaster recovery plans by providing more complete coverage of contingency issues, selecting more realistic test and/or exercise scenarios and environments, and more effectively stressing the information system and supported missions.

(4) The organization exercises this plan on a semiannual basis.

LOW CP-4*	**MOD** CP-4 (1)*	**HIGH** CP-4 (1)*

CP-5 CONTINGENCY DISASTER RECOVERY PLAN UPDATE

Control: Review the contingency and disaster recovery plans for the information system at least annually and revise the plan to address system and/or organizational changes or problems encountered during plan implementation, execution, or testing.

Supplemental Guidance: Organizational changes include changes in mission, functions, or business processes supported by the information system.

Control Enhancements: None.

LOW CP-5	**MOD** CP-5	**HIGH** CP-5

CP-6 ALTERNATE STORAGE SITE

Control: If required by the system owners and the Business Impact Analysis, identify an alternate storage site and initiate necessary agreements to permit the storage of information system backup information. Ensure that the frequency of information system backups and the transfer rate of backup information to the alternate storage site (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives.

Control Enhancements:

(1) The organization identifies an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards.

(2) The organization configures the alternate storage site to facilitate timely and effective recovery operations.

(3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

(4) The organization performs daily data backups and stores recovery media offsite at a location that affords protection of the data in accordance with its confidentiality, integrity, and availability levels.

(5) The organization accomplishes data backup by maintaining a redundant secondary system, not collocated, that can be activated without loss of data or disruption to the operation.

(6) The organization will consider alternative procedures, such as secure transmission of the data to an appropriate offsite location if regular offsite backup is not feasible.

LOW Not Required	**MOD** CP-6 (1)(3)	**HIGH** CP-6 (1)(2)(3)(4)(5)

CP-7 ALTERNATE PROCESSING SITE

Control: If required by the Business Impact Analysis, identify an alternate processing site and initiate necessary agreements to permit the resumption of information system operations for critical mission and/or business functions within the organization-defined time period when the primary processing capabilities are unavailable. Ensure that the timeframes to resume information system operations are consistent with organization-established recovery time objectives.

Supplemental Guidance: None

Control Enhancements:

(1) The organization identifies an alternate processing site that is geographically separated from the primary processing site so as not to be susceptible to the same hazards.

(2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

(3) The organization develops alternate processing site agreements that contain priority-of--service provisions in accordance with the organization's availability requirements.

(4) The organization fully configures the alternate processing site so that it is ready to be used as the operational site supporting a minimum required operational capability.

(5) The organization ensures that the alternate site provides security measures, to include boundary defense and user connectivity and access controls, equivalent to the primary site.

LOW	Not Required	**MOD**	CP-7 (1)(2)(3)	**HIGH**	CP-7 (1)(2)(3)(4)(5)

CP-8 TELECOMMUNICATIONS SERVICES

Control: Identify primary and alternate telecommunications services to support the information system and initiate necessary agreements to permit the resumption of system operations for critical mission and/or business functions in a timely manner, as specified by the operating unit, when the primary telecommunications capabilities are unavailable.

Supplemental Guidance: In the event that the primary and/or alternate telecommunications services are provided by a common carrier, the organization requests Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness.

Control Enhancements:

(1) The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

(2) The organization obtains alternate telecommunications services that do not share a single point of failure with primary telecommunications services.

(3) The organization obtains alternate telecommunications service providers that are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.

(4) The organization requires primary and alternate telecommunications service providers to have adequate contingency plans.

LOW	Not Required	**MOD**	CP-8 (1)	**HIGH**	CP-8 (1)(2)(3)(4)

CP-9 INFORMATION SYSTEM BACKUP

Control: Conduct backups of user-level and system-level information (including system state information) contained in the information system at least annually and store backup information at an appropriately secured location if required by the Business Impact Analysis. The NNSA Element ensures that the frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives.

Supplemental Guidance: While integrity and availability are the primary concerns for system backup information, protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the backup media and the associated risk level. An organizational assessment of risk guides the use of encryption for backup information. The protection of system backup information while in transit is beyond the scope of this control. Related security controls: MP4 and MP5.

Control Enhancements:

(1) The organization tests backup information annually to verify media reliability and information integrity.

(2) The organization selectively uses backup information in the restoration of information system functions as part of contingency plan and disaster recovery testing.

(3) The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.

(4) The organization protects system backup information from unauthorized modification. The organization employs appropriate mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of information system backups.

LOW CP-9	**MOD** CP-9 (1)(4)	**HIGH** CP-9 (1)(2)(3)(4)

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Control: Employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.

Control Enhancements:

(1) The organization includes a full recovery and reconstitution of the information system as part of contingency plan and disaster recovery testing.

(2) The organization documents circumstances that can inhibit a recovery to a known, secure state and implements the appropriate mitigating controls.

(3) Information systems that are transaction-based (e.g., database management systems, transaction processing systems) will implement transaction rollback and transaction journaling, or technical equivalents.

LOW CP-10 (2)	**MOD** CP-10 (1)(2)	**HIGH** CP-10 (1)(2)(3)

FAMILY: IDENTIFICATION AND AUTHENTICATION CLASS: TECHNICAL

Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an information system. Access control usually requires that the system be able to identify and differentiate among users. All NNSA information systems must have a means to enforce user accountability, so that system activity (both authorized and unauthorized) can be traced to a specific user. To facilitate user accountability, all information systems must implement a method of user identification and authentication. The user identification tells the system who the user is. The authentication mechanism provides an added level of assurance that the user really is who they say they are. Authentication consists of something a user knows (such as a password), something the user has (such as a token or smart card), or something the user is (such as a fingerprint). User identification and authentication also can enforce separation of duties.

The following is NNSA policy:

- All information systems require distinct user IDs that are unique to each user or group for user identification.
- All information systems require an authentication mechanism that is unique to each user or group, such as but not limited to; passwords, one-time passwords, biometrics, or public-key infrastructure certificates for primary access to all information and information system resources. The implementation or technology used should provide access security commensurate with the level of sensitivity assigned to the resource (i.e., information, devices or systems).
- All information systems and associated equipment that rely on passwords as the means to authenticate users must implement effective password management in accordance with the Element's CSPP.

Identification and Authentication				
Control Number	**Control Name**	**Control Baselines**		
		Low	Moderate	High

Identification and Authentication				
Control Number	**Control Name**	**Control Baselines**		
		Low	Moderate	High
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1
IA-2	User Identification and Authentication	IA-2 (1)(4)	IA-2 (2)(3)(4)(5)	IA-2 (2)(3)(4)(5)
IA-3	Device Identification and Authentication	Not Required	IA-3 (1) IA-3	IA-3 (2) IA-3
IA-4	Identifier Management	IA-4	IA-4 (1)(2)	IA-4 (1)(2)
IA-5	Authenticator Management	IA-5 (1)(2)(3)(4)	IA-5 (1)(2)(3)(4)	IA-5 (1)(2)(3)(4)(5)
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control: Develop, disseminate, and periodically review and update:

a. A formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Supplemental Guidance: Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators where technically feasible.

Control Enhancements: None.

LOW IA-1	**MOD** IA-1	**HIGH** IA-1

IA-2 USER IDENTIFICATION AND AUTHENTICATION

Control: Uniquely identify and authenticate users (or processes acting on behalf of users) on all information systems, where technically feasible.

Supplemental Guidance: Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Local access is any access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network. Related security controls: AC-14 and AC-17.

Control Enhancements:

(1) The information system employs passwords and/or PINs for local and remote system access.

(2) The information systems employ a multifactor authentication process or device that generates a onetime password, for local system access.

Enhancement Supplemental Guidance: Multifactor authentication could include soft tokens, hard tokens, scratch card, or grid cards, that generate one time passwords. One time passwords could include the type one gets from time synchronous devices (e.g., SecurID) from challenge response devices, or from the protocol handshake that underlies PKI.

(3) The information system employs a multifactor authentication process or device, that generates a onetime password, for remote system access, where one of the factors is separate from the system being used to gain access.

Enhancement Supplemental Guidance: The additional phrase is intended to eliminate concepts such as soft tokens. This is intended to address an OMB0616 requirement for remotely accessing systems containing PII, (there is no NSS exception).

(4) If passwords and/or PINs are employed they shall be compliant with the Element's CSPP..

(5) If certificate-based authentication is employed it shall be compliant with the applicable control enhancements in IA5.

LOW IA-2 (1)(4)	**MOD** IA-2 (2)(3)(4)(5)	**HIGH** IA-2 (2)(3)(4)(5)

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system identifies and authenticates specific devices before establishing a connection.

Supplemental Guidance: The information system typically uses either shared known information (e.g., physical address or TCP/IP address), organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the LoC of the information system with higher risk levels requiring stronger authentication. For remote access via VPN, the VPN server is considered the information system which handles the identification and authentication of remote devices.

Control Enhancements:

(1) The information system employs bidirectional authentication that is cryptographically based between devices before establishing remote communication connections.

(2) The information system employs bidirectional authentication that is cryptographically based (or uses authorized PTS) between devices before establishing remote or local communication connections.

LOW	Not Required	**MOD**	IA-3 (1)	**HIGH**	IA-3 (2)
LOW	Not Required	**MOD**	IA-3	**HIGH**	IA-3

IA-4 IDENTIFIER MANAGEMENT

Control: Manage user identifiers by:

a. Uniquely identifying each user;

b. Verifying the identity of each user;

c. Receiving authorization to issue a user identifier from an appropriate organization official;

d. Issuing the user identifier to the intended party;

e. Disabling the user identifier after the period of inactivity noted in the site CSPP; and

f. Archiving user identifiers.

g. Establish separate unique identifier for privileged accounts and actions.

Supplemental Guidance: Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts).

Control Enhancements:

(1) NNSA Elements require that registration to receive a user ID include authorization by a supervisor or sponsor (or management designee), and be done in person before a designated registration authority.

(2) The organization requires documentary evidence of a user's identity to be presented to the registration authority.

LOW IA-4	**MOD** IA-4 (1)(2)	**HIGH** IA-4 (1)(2)

IA-5 AUTHENTICATOR MANAGEMENT

Control: Manage information system authenticators by:

a. Defining initial authenticator content;

b. Establishing administrative procedures for initial authenticator distribution, for lost and/or compromised, or damaged authenticators, and for revoking authenticators;

c. Changing default authenticators upon information system installation; and

d. Changing and/or refreshing authenticators at least annually

Supplemental Guidance: Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Complies with all applicable laws, statutes, national policies and related E-authentication initiatives, authentication of public users accessing Federal information systems (and associated authenticator management) may also be required to protect nonpublic or privacy-related information.

Control Enhancements:

(1) Information systems utilizing a logon ID and password for user identification and authentication enforce the following for reusable passwords:

(a) Password complexity is not less than a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters (one of which must be in the first seven positions), including at least one of each (e.g., emPagd2!). (Document in a system's ISSP if a system is incapable of meeting this requirement.)

(b) At least four characters must be changed when a new password is created.

(c) Passwords are encrypted both for storage and for transmission, where technically feasible.

(d) Enforces password minimum and maximum lifetime restrictions; and

(e) Prohibits password reuse for a specified number [NNSA Element defined] of generations.

Enhancement Supplemental Guidance: Deployed/tactical systems with limited data input capabilities implement the password policy to the extent possible.

(2) The organization ensures that passwords are protected commensurate with the classification or sensitivity of the information accessed.

(3) The organization ensures that policy prohibits passwords from being embedded in access scripts or stored on function keys.

(4) Information systems utilizing PKI-based authentication:

(a) Validates certificates by constructing a certification path to a trusted certificate authority;

(b) Establishes user control of the corresponding private key; and

(c) Maps the authenticated identity to the user account.

(5) The organization employs automated tools to validate that the passwords are sufficiently strong to resist cracking and other types of attacks intended to discover a user's password.

Enhancement Supplemental Guidance: These tools may only be employed under the auspices of the DAA. This type of testing can be accomplished in association with RA5.

LOW IA-5 (1)(2)(3)(4)	**MOD** IA-5 (1)(2)(3)(4)	**HIGH** IA-5 (1)(2)(3)(4)(5)

IA-6 AUTHENTICATOR FEEDBACK

Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance: The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication

mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information

Control Enhancements: None.

LOW IA-6	**MOD** IA-6	**HIGH** IA-6

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: If used, the information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Supplemental Guidance: None.

Control Enhancements: None.

LOW IA-7	**MOD** IA-7	**HIGH** IA-7

FAMILY: INCIDENT RESPONSE CLASS: OPERATIONAL

An incident response capability is a mechanism through which an NNSA Element's system owners and Information System Security Officers are kept informed of system vulnerability advisories from the US-Computer Emergency Readiness Team (US-CERT), software vendors, and other sources. The capability also coordinates with responsible incident response capabilities regarding the handling and reporting of incidents involving systems under the NNSA Element's responsibility. An incident response capability may consist of one or more persons (such as the Information System Security Officer or CIO), who ensure that vulnerability advisories are communicated to system owners.

Incident Response				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1
IR-2	Incident Response Training	IR-2	IR-2	IR-2 (1)(2)
IR-3	Incident Response Testing	Not Required	IR-3	IR-3 (1)

Incident Response				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	IR-5	IR-5 (1)	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (1)	IR-7 (1)

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control: Develop, disseminate, and periodically review/update:

a. A formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Supplemental Guidance: The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required.

Control Enhancement: None

LOW IR-1	**MOD** IR-1	**HIGH** IR-1

IR-2 INCIDENT RESPONSE TRAINING

Control: Train personnel in their incident response roles and responsibilities with respect to the information system and provide refresher training at least annually.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

(2) The organization employs automate mechanisms to provide a more thorough and realistic training environment.

LOW IR-2	**MOD** IR-2	**HIGH** IR-2 (1)(2)

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES

Control: Test and/or exercise the incident response capability for the information system at least annually using the tests and exercises defined in the ISSP to determine the incident response effectiveness and document the results.

Supplemental Guidance: None

Control Enhancements:

(1) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.

Enhancement Supplemental Guidance: Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the capability by providing more complete coverage of incident response issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the response capability.

LOW IR-3	**MOD** IR-3	**HIGH** IR-3 (1)

IR-4 INCIDENT HANDLING

Control: Implement an incident handling capability for security incidents that includes preparation, detection and analysis, evidence preservation, containment, eradication, and recovery.

Supplemental Guidance: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related security controls: AU-6 and PE-6.

Control Enhancement:

(1) The organization employs automated mechanisms to support the incident handling process.

LOW IR-4	**MOD** IR-4 (1)	**HIGH** IR-4 (1)

IR-5 INCIDENT MONITORING

Control: Track and document information system security incidents on an ongoing basis.

Supplemental Guidance: None.

Control Enhancement:

(1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

LOW IR-5	**MOD** IR-5 (1)	**HIGH** IR-5 (1)

IR-6 INCIDENT REPORTING

Control: Promptly report incident information to appropriate authorities.

Supplemental Guidance: The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consisted with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. In addition to incident information, weaknesses and vulnerabilities in the information system are reports to appropriate organizational officials in a timely manner to prevent security incidents.

Control Enhancement:

(1) The organization employs automated mechanisms to assist in the reporting of security incidents.

LOW IR-6	**MOD** IR-6 (1)	**HIGH** IR-6 (1)

IR-7 INCIDENT RESPONSE ASSISTANCE

Control: Provide an incident response support resource (internal or external incident response capability support) that offers advice and assistance to users of the information systems for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.

Supplemental Guidance: Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required.

Control Enhancement:

(1) The organization employs automated mechanisms to increase the availability of incident response related information and support.

LOW IR-7	**MOD** IR-7 (1)	**HIGH** IR-7 (1)

FAMILY: MAINTENANCE CLASS: OPERATIONAL

These are controls to ensure that maintenance activities are controlled and monitored to ensure that the confidentiality, integrity or availability of the information is not compromised.

Maintenance				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1
MA-2	Periodic Maintenance	MA-2	MA-2 (1)	MA-2 (1) (2)
MA-3	Maintenance Tools	MA-3 (2)	MA-3 (1)(2)(3)(4)	MA-3 (1)(2)(3)(4)
MA-4	Remote Maintenance	MA-4 (1)(2)(3)(4)	MA-4 (1)(2)(3)(4)	MA-4 (1)(2)(3)(4)(5)
MA-5	Maintenance Personnel	MA-5 (1)(4)	MA-5 (1)(2)(3)(4)	MA-5 (1)(2)(3)(4)
MA-6	Timely Maintenance	Not Required	MA-6 (1)	MA-6 (2)

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control: Develop, disseminate, and periodically review/update:

a. A formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

Supplemental Guidance: The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance

procedures can be developed for the security program in general, and for a particular information system, when required.

Control Enhancements: None.

LOW MA-1	**MOD** MA-1	**HIGH** MA-1

MA-2 CONTROLLED MAINTENANCE

Control:

a. The organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

b. All maintenance activities to include routine, scheduled maintenance and repairs are controlled; whether performed on site or remotely and whether the equipment is serviced on site or removed to another location.

c. The ISSM approves the removal of information system or information system components that processed sensitive or classified information from the site when repairs are necessary.

d. If the information system or component of the system requires offsite repair, the organization removes all information from associated media using approved procedures.

e. After maintenance is performed on the information system, the organization checks all potentially impacted security controls to verify that the controls are still functioning properly.

Supplemental Guidance: None

Control Enhancements:

(1) The organization maintains maintenance records for the information system that include:

(a) The date and time of maintenance;

(b) Name of the individual performing the maintenance;

(c) Name of escort, if necessary;

(d) A description of the maintenance performed; and

(e) A list of equipment removed or replaced (including identification numbers, if applicable).

(2) The organization employs automated mechanisms to schedule and conduct maintenance as required, and to create up-to-date, accurate, complete, and available records of all maintenance actions, both needed and completed.

LOW MA-2	**MOD** MA-2 (1)	**HIGH** MA-2 (1)(2)

MA-3 MAINTENANCE TOOLS

Control: Approve, control, and monitor the use of information system maintenance tools and maintain the tools on an ongoing basis.

Supplemental Guidance: The intent of this control is to address hardware and software brought into the information system specifically for diagnostic/repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control.

Control Enhancements:

(1) The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.

Enhancement Supplemental Guidance: Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.

(2) The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.

(3) The organization checks all maintenance equipment with the capability of retaining information so that no organizational information is written on the equipment or the equipment is appropriately sanitized before release. In the event the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.

Enhancement Supplemental Guidance: The National Security Agency provides a listing of approved media sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

(4) The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.

LOW	MA-3 (2)	**MOD**	MA-3 (1)(2)(3)(4)	**HIGH**	MA-3 (1)(2)(3)(4)

MA-4 REMOTE MAINTENANCE

Control: Remote maintenance and diagnostics of classified systems must be approved by the CSPM.

a. Authorize, monitor, and control any remotely executed maintenance and diagnostic activities, if employed.

b. Ensure that the use of remote maintenance and diagnostic tools is consistent with NNSA policy.

c. Maintain records for all remote maintenance and diagnostic activities.

d. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections invoked in the performance of that activity.

Supplemental Guidance: Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, untrusted resource (e.g., dial-up connections and the Internet). Related security controls: IA2, MP6.

Control Enhancements:

(1) The organization audits all remote maintenance and diagnostic sessions and appropriate organizational personnel review the maintenance records of the remote sessions.

(2) The organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the information system.

(3) The organization does not allow remote maintenance or diagnostic services to be performed by a provider that does not implement for its own information system, a level of protection at least as high as that implemented on the system being serviced.

Enhancement Supplemental Guidance: The organization should consider the following aspects depending upon the maintenance provider: (i) Removal and sanitization of the information system component prior to service. (ii) An inspection of the information system component should be accomplished prior to reconnecting the component to the information system to address vulnerabilities (e.g., malicious software and surreptitious implants).

(4) If password based authentication is used to accomplish remote maintenance, the organization changes the passwords following each remote maintenance service.

(5) When remote administration and maintenance of an information system is employed, the organization requires that the session is protected through the use of a strong authenticator tightly bound to the user (e.g., PKI where certificates are stored on a token protected by a password, pass-phrase or biometric); AND EITHER;

(a) Physically separate communications paths, OR

(b) Logically separated communications paths based upon EITHER

1) NSA-approved cryptographic mechanisms used to protect classified information from individuals who lack the necessary clearance; OR

2) DAA-approved cryptographic mechanisms (in consultation with the data steward) to separate compartments or provide need-to-know protection

LOW MA-4 (1)(2)(3)(4)	**MOD** MA-4 (1)(2)(3)(4)	**HIGH** IMA-4 (1)(2)(3)(4)(5)

MA-5 MAINTENANCE PERSONNEL

Control: Maintain a list of personnel authorized to perform maintenance on the information system. Only authorized personnel perform maintenance on the information system.

Supplemental Guidance: Maintenance personnel (whether performing maintenance locally or remotely) have appropriate access authorizations to the information system when maintenance activities allow access to organizational information.

Control Enhancements:

(1) The organization establishes and documents the processes for maintenance personnel authorization.

(2) Personnel who perform maintenance on classified National Security Systems must be cleared to the highest level of information on the system.

Enhancement Supplemental Guidance: In the event that appropriately cleared personnel are unavailable to perform maintenance, an uncleared person, or one cleared to a lower level, may be used once provided a fully cleared and technically qualified escort.

(3) Personnel who perform maintenance on National Security Systems should be US citizens.

(4) Procedures for the use of maintenance personnel that are uncleared, lower cleared or Non-US citizens shall be outlined in the approved system security plan and at a minimum address the following requirements:

(a) Maintenance personnel who do not have needed access authorizations; clearances or formal access approvals shall be escorted and supervised by approved organizational personnel with appropriate access authorizations during the performance of maintenance activities on the information system.

(b) Prior to maintenance by personnel who do not have needed access authorizations; clearances or formal access approvals, all volatile data storage components of the information system shall be completely sanitized and all nonvolatile data storage media shall be completely removed or physically disconnected and secured.

Enhancement Supplemental Guidance: In the event a system cannot be sanitized, the procedures contained in the approved system security plan shall be enforced. The primary intent of this control is to deny the uncleared or lower-cleared individual visual and electronic access to any classified or sensitive information contained on the system.

(5) Cleared foreign nationals may be utilized as maintenance personnel for those systems jointly owned and operated by the US and foreign allied governments, or those owned and operated by foreign allied governments. Approvals, consents, and detailed operational conditions must be fully documented within a Memorandum of Agreement.

LOW MA-5 (1)(4)	**MOD** MA-5 (1)(2)(3)(4)	**HIGH** MA-5 (1)(2)(3)(4)

MA-6 TIMELY MAINTENANCE

Control: Obtain maintenance support and spare parts for key information system components within a time frame to support mission requirement following a failure.

Supplemental Guidance: None

Control Enhancements:

(1) The organization ensures that key IT assets are identified, and that maintenance support for them, to include maintenance spares and spare parts, is available to respond within 24 hours of failure.

(2) The organization ensures that key IT assets are identified, and that maintenance support for them, to include maintenance spares and spare parts, is available to respond 24 x 7 immediately upon failure.

LOW Not Required	**MOD** MA-6 (1)	**HIGH** MA-6 (2)

FAMILY: MEDIA PROTECTION CLASS: OPERATIONAL

NNSA requires that NNSA Element cyber security programs include procedures for storing, handling, and destroying national and non-national security information media.

Media Protection				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2(1)	MP-2 (1)
MP-3	Media Labeling	MP-3 (1)	MP-3 (1)(2)	MP-3 (1)(2)
MP-4	Media Storage	MP-4 (1)(2)	MP-4 (1)(2)	MP-4 (1)(2)
MP-5	Media Transport	MP-5 (1)	MP-5 (1)(2)	MP-5 (1)(2)(3)
MP-6	Media Sanitization and Disposal	MP-6 (1)	MP-6 (1)(2)(3)	MP-6 (1)(2)(3)

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Control: Develop, disseminate, and periodically review/update:

a. A formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

Supplemental Guidance: The media protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general, and for a particular information system, when required.

Control Enhancements: None.

LOW MP-1	**MOD** MP-1	**HIGH** MP-1

MP-2 MEDIA ACCESS

Control: Restrict access to information system media to authorized individuals. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access.

Supplemental Guidance: Information system media includes digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks). This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).

Control Enhancement:

(1) Unless guard stations control access to media storage areas, the organization employs mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

Enhancement Supplemental Guidance: This control enhancement is primarily applicable to designated media storage areas within an organization where a significant volume of media is stored and is not intended to apply to every location where some media is stored (e.g., in individual offices).

LOW MP-2	**MOD** MP-2 (1)	**HIGH** MP-2 (1)

MP-3 MEDIA LABELING

Control:

a. Mark removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information. Note that this requirement should be limited to media and paper output, and only to information requiring special handling, such as PII, UCNI, or classified media.

b. Specific types of media identified in the site's CSPP or in the ISSP for the system may be exempt from labeling so long as they remain within a secure environment.

c. Organizations document in policy and procedures, the media requiring labeling and the specific measures taken to afford such protection.

Supplemental Guidance: An organizational assessment of risk guides the selection of media requiring labeling. The rigor with which this control is applied is commensurate with the security categorization of the information contained on the media. For example, labeling is not required for media containing information determined by the organization to be in the public domain or to be publicly releasable.

Control Enhancement:

1. The information system shall mark human-readable output appropriately on each human-readable page, screen, or equivalent.

2. In facilities where some of the information systems are operated as classified and some are dedicated to unclassified operation, removable unclassified media must be uniquely marked to prevent them from being mixed with classified media.

LOW MP-3 (1)	**MOD** MP-3 (1)(2)	**HIGH** MP-3 (1)(2)

MP-4 MEDIA STORAGE

Control:

a. Physically control and securely store information system media within controlled areas.

b. Document in policy and procedures, the media requiring physical protection and the specific measures taken to afford such protection.

c. Protect information system media identified by the organization until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Telephony systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems. An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or

individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection. As part of a defense-in-depth protection strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. Related security controls: CP9 and RA2.

Control Enhancements:

(1) At the discretion of the data custodian the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information at rest unless otherwise protected by alternative physical protection measures. The strength of the cryptographic mechanism is commensurate with the classification and sensitivity of the information:

(a) The information system uses FIPS-certified cryptography to encrypt sensitive or controlled unclassified data at rest. See Chapter VII for requirements regarding Sensitive Unclassified Information.

(b) The information system uses NSA-approved cryptography to encrypt classified information at rest.

Enhancement Supplemental Guidance: The selection and strength of cryptographic mechanisms is based upon maintaining the confidentiality of the information (i.e., a lack of user clearance and/or need to know).

(2) The organization implements effective cryptographic key management in support of secondary storage encryption and provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.

LOW MP-4 (1)(2)	**MOD** MP-4 (1)(2)	**HIGH** MP-4 (1)(2)

MP-5 MEDIA TRANSPORT

Control: Protect and control information system media and restrict the pickup, transfer, and delivery of such media to authorized personnel. Document in policy and procedures, the media requiring protection during transport and the specific measures taken to protect such transported media. All classified media must be destroyed. In addition, nothing is released outside of DOE once surplused, and is also must be destroyed.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, and digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This

control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones) that are transported outside of controlled areas. Telephone systems are also information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. An organizational assessment of risk guides the selection of media and associated information contained on that media requiring protection during transport.
The rigor with which this control is applied is commensurate with the security categorization of the information contained on the media. An organizational assessment of risk also guides the selection and use of appropriate storage containers for transporting non-digital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service).

Control Enhancements:

(1) The organization protects digital media during transport outside of controlled areas using organization approved physical and technical security measures commensurate with the classification and sensitivity of the information residing on the media, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

(2) The organization employs an identified custodian at all times to transport information system media.

(3) At the discretion of the data custodian, the organization employs cryptographic mechanisms commensurate with the classification and sensitivity of the information residing on the media.

Enhancement Supplemental Guidance: Cryptographic mechanisms support the confidentiality and/or integrity security objectives. Cryptographic mechanisms prevent unauthorized disclosure of information during transport. Related control MP-4 (2).

LOW MP-5 (1)	**MOD** MP-5 (1)(2)	**HIGH** MP-5 (1)(2)(3)

MP-6 MEDIA SANITIZATION AND DISPOSAL

Control: The organization sanitizes information system media, , prior to disposal or release for reuse.

Supplemental Guidance: Sanitization is the process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed.

Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or disposed. The organization uses its discretion on sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposed. The National Security Agency also provides media sanitization guidance and maintains a listing of approved sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

Control Enhancements:

(1) The organization tracks, documents, and verifies media sanitization and disposal actions.

(2) The organization periodically tests sanitization equipment and procedures to verify correct performance.

(3) The organization ensures that all information technology equipment and machine-readable media are cleared and sanitized according to NAP 14.1-C before being released outside of organizational control. The strength and integrity of the clearing/sanitization mechanism is commensurate with the classification and sensitivity of the information:

(a) Information technology equipment and media containing controlled unclassified data are cleared and sanitized according to applicable organizational or national standards.

(b) Information technology equipment and media containing classified data are cleared and sanitized according organizational or national standards.

LOW MP-6 (1)	**MOD** MP-6 (1)(2)(3)	**HIGH** MP-6 (1)(2)(3)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION CLASS: OPERATIONAL

The information and information resources that must be physically protected, in order to ensure that security objectives are met, will be located within controlled access facilities that mitigate unauthorized physical access. The information and information system resources must be physically protected in accordance with NNSA and site policies and procedures.

Physical and Environmental Protection				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
PE-1	Physical and Environmental	PE-1	PE-1	PE-1

Physical and Environmental Protection				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
	Protection Policy and Procedures			
PE-2	Physical Access Authorizations	PE-2 (1)(2)	PE-2(1)(2)	PE-2(1)(2)
PE-3	Physical Access Control	PE-3 (1)	PE-3 (1)(2)	PE-3 (1)(2)
PE-4	Access Control for Transmission Medium	Not Required	PE-4	PE-4
PE-5	Access Control for Display Medium	PE-5	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6 (1)	PE-6 (1) (2)
PE-7	Visitor Control	PE-7 (1)	PE-7 (1)	PE-7 (1)
PE-8	Access Records	PE-8	PE-8	PE-8
PE-9	Power Equipment and Power Cabling	Not Required	PE-9	PE-9 (1)(2)
PE-10	Emergency Shutoff	Not Required	PE-10 (1)	PE-10 (1)
PE-11	Emergency Power	Not Required	PE-11	PE-11 (1)
PE-12	Emergency Lighting	PE-12	PE-12 (1)	PE-12 (1)
PE-13	Fire Protection	PE-13 (4)	PE-13 (1)(4)	PE-13 (1)(2)(3)(4)
PE-14	Temperature and Humidity Controls	PE-14	PE-14 (1)	PE-14 (1)
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Required	PE-17	PE-17
PE-18	Location of Information System Components	Not Required	PE-18	PE-18(1)
PE-19	Information Leakage *(Classified Systems Only)*	Not Required	PE-19 (1)	PE-19 (1)

Physical and Environmental Protection				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
PE-20	Physical Security	Not Required	PE-20 (1)(2)(3)	PE-20 (1)(2)(3)
PE-21	Environmental Control Training	Not Required	PE-21	PE-21

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control: Develop, disseminate, and periodically review/update:

a. A formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

Supplemental Guidance: The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general, and for a particular information system, when required.

Control Enhancements: None.

LOW PE-1	**MOD** PE-1	**HIGH** PE-1

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control:

a. Develop and keep current a list of personnel with authorized access to facilities containing information systems (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials.

b. Designated officials within the organization review and approve the access list and authorization credentials at least annually.

Supplemental Guidance: Appropriate authorization credentials include, for example, badges, identification cards, and smart cards. The organization promptly removes

from the access list personnel no longer requiring access to the facility where the information system resides.

Control Enhancements:

(1) The organization controls physical access to computing facilities that process controlled unclassified information on a need-to-know basis.

Enhancement Supplemental Guidance: Organizational position or role may be sufficient to dynamically establish need-to-know.

(2) The organization limits physical access to computing facilities that process classified information to authorized personnel with appropriate clearances and need-to-know.

LOW PE-2 (1)(2)	**MOD** PE-2 (1)(2)	**HIGH** PE-2 (1)(2)

PE-3 PHYSICAL ACCESS CONTROL

Control: Control all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facility officially designated as publicly accessible) and verify individual access authorizations before granting access to the facility. Each NNSA Element must also control access to areas officially designated as publicly accessible, as appropriate, in accordance with the Element's assessment of risk.

Supplemental Guidance: The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys: (i) periodically; and (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled.

Control Enhancements:

(1) The organization controls physical access to the information system independent of the physical access controls for the facility.

Enhancement Supplemental Guidance: This control enhancement, in general, applies to server rooms, communications centers, or any other areas within a facility containing large concentrations of information system components or components with a higher impact level than that of the majority of the facility. The intent is to provide an additional layer of physical security for those areas where the organization may be more vulnerable due to the concentration of information system components or the impact

level of the components. The control enhancement is not intended to apply to workstations or peripheral devices that are typically dispersed throughout the facility and used routinely by organizational personnel.

(2) The organization ensures that every physical access point to facilities housing workstations that store or display classified information is guarded or alarmed when unattended.

LOW PE-3 (1)	**MOD** PE-3 (1)(2)	**HIGH** PE-3 (1)(2)

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: Control physical access to information system distribution and transmission lines carrying unencrypted information to prevent eavesdropping, in-transit modification, disruption, or physical tampering.

Supplemental Guidance: Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

Control Enhancements: None.

LOW Not Required	**MOD** PE-4	**HIGH** PE-4

PE-5 ACCESS CONTROL FOR DISPLAY MEDIUM

Control: Control physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.

Supplemental Guidance: None

Control Enhancements: None.

LOW PE-5	**MOD** PE-5	**HIGH** PE-5

PE-6 MONITORING PHYSICAL ACCESS

Control: Monitor physical access to the information system to detect and respond to physical security incidents.

Supplemental Guidance: The organization reviews physical access logs periodically and investigates apparent security violations or suspicious physical access activities. Response to detected physical security incidents is part of the organization's incident response capability.

Control Enhancements: `

(1) The organization monitors real-time physical intrusion alarms and surveillance equipment.

(2) The organization employs automated mechanisms to recognize potential intrusions and initiate appropriate response actions.

LOW PE-6	**MOD** PE-6 (1)	**HIGH** PE-6 (1)(2)

PE-7 VISITOR CONTROL

Control: Control physical access to the information system by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible.

Supplemental Guidance: Government contractors and others with permanent authorization credentials are not considered visitors.

Control Enhancements:

(1) The organization escorts visitors and monitors visitor activity.

LOW PE-7 (1)	**MOD** PE-7 (1)	**HIGH** PE-7 (1)

PE-8 ACCESS RECORDS

Control: Ensure visitor access records to sites (except for those areas within the sites officially designated as publicly accessible) are maintained in accordance with NNSA requirements.

Supplemental Guidance: None

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the maintenance and review of access records.

(2) The organization maintains a record of all physical access, both visitor and authorized individuals.

LOW PE-8	**MOD** PE-8	**HIGH** PE-8

PE-9 POWER EQUIPMENT AND POWER CABLING

Control: Ensure power equipment and power cabling for the information systems are protected from damage and destruction.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs redundant and parallel power cabling paths to the information system.

(2) The organization will employ automatic voltage control for key IT assets.

LOW Not Required	**MOD** PE-9	**HIGH** PE-9 (1)(2)

PE-10 EMERGENCY SHUTOFF

Control: Provide the capability of shutting off primary power for computer room equipment that may be malfunctioning or threatened, without endangering personnel by requiring them to approach the equipment.

Supplemental Guidance: Facilities containing concentrations of information system resources may include, for example, data centers, server rooms, and mainframe rooms.

Control Enhancement:

(1) The organization protects the emergency power-off capability from accidental or unauthorized activation.

LOW Not Required	**MOD** PE-10 (1)	**HIGH** PE-10 (1)

PE-11 EMERGENCY POWER

Control: Ensure a short-term uninterruptible power supply facilitates an orderly shutdown of the information system (in accordance with its ISSP) in the event of an unanticipated primary power source loss. This determination is made by the system owner.

Supplemental Guidance: None.

Control Enhancements:

(1) The NNSA Element provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

LOW Not Required	**MOD** PE-11	**HIGH** PE-11 (1)

PE-12 EMERGENCY LIGHTING

Control: Ensure automatic emergency lighting is employed and maintained that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.

Supplemental Guidance: None.

Control Enhancement:

(1) The organization provides emergency lighting for all areas necessary to maintain mission or business essential functions.

LOW PE-12	**MOD** PE-12 (1)	**HIGH** PE-12 (1)

PE-13 FIRE PROTECTION

Control: Ensure fire suppression and detection devices/systems are employed and maintained that can be activated in the event of a fire.

Supplemental Guidance: Fire suppression and detection devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Control Enhancements:

(1) The NNSA Element employs fire detection devices/systems that activate automatically and notify the organization and emergency responders in the event of a fire.

(2) The NNSA Element employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders.

(3) The NNSA Element employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.

(4) The NNSA Element ensures that computing facilities undergo a periodic fire marshal inspection, and promptly resolves identified deficiencies.

LOW PE-13 (4)	**MOD** PE-13 (1)(4)	**HIGH** PE-13 (1)(2)(3)(4)

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: Ensure the temperature and humidity within facilities containing information systems are regularly maintained and monitored, within acceptable levels.

Supplemental Guidance: None.

Control Enhancement:

(1) The organization installs automatic humidity and temperature controls in computing facilities to prevent potentially harmful fluctuations.

LOW PE-14	**MOD** PE-14 (1)	**HIGH** PE-14 (1)

PE-15 WATER DAMAGE PROTECTION

Control: Ensure the information system is protected from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves that are accessible, working properly, and known to key personnel.

Supplemental Guidance: None.

Control Enhancement:

(1) The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a significant water leak.

LOW PE-15	**MOD** PE-15	**HIGH** PE-15 (1)

PE-16 DELIVERY AND REMOVAL

Control: Ensure information system-related items (i.e., hardware, firmware, software) entering and exiting the site are authorized and controlled, and that appropriate records of those items are maintained.

Supplemental Guidance: The organization controls delivery areas and, if possible, isolates the areas from the information system and media libraries to avoid unauthorized physical access. Related control MP-6.

Control Enhancements: None.

LOW PE-16	**MOD** PE-16	**HIGH** PE-16

PE-17 ALTERNATE WORK SITE

Control: Require that individuals within the operating unit employ appropriate management, operational, and technical information system security controls at alternate work sites.

Supplemental Guidance: The organization provides a means for employees to communicate with information system security staff in case of security problems.

Control Enhancements: None.

LOW Not Required	**MOD** PE-17	**HIGH** PE-17

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

Control: Ensure information system components are positioned within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards.

Control Enhancement:

(1) The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

LOW Not Required	**MOD** PE-18	**HIGH** PE-18 (1)

PE-19 INFORMATION LEAKAGE

Control: Ensure the information system is protected from information leakage due to electromagnetic signals emanations (classified systems only).

Supplemental Guidance: The security categorization (for confidentiality) of the information system and organizational security policy guides the application of safeguards and countermeasures employed to protect the information system against information leakage due to electromagnetic signals emanations.

Control Enhancements:

(1) The organization ensures that components of the systems, associated data communications, and networks shall be protected in accordance with national emissions and TEMPEST policies and procedures applicable to the sensitivity level of the data being transmitted.

LOW Not Required	**MOD** PE-19 (1)	**HIGH** PE-19 (1)

PE-20 PHYSICAL SECURITY

Control: Ensure that information and equipment are deployed or stored in approved facilities or containers with documented accountability procedures.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization periodically tests the physical security of key computing facilities.

(2) The organization implements procedures that ensure the proper handling and storage of information.

(3) The organization provides employees with periodic training in the operation of physical security controls.

LOW Not Required	**MOD** PE-20 (1)(2)(3)	**HIGH** PE-20 (1)(2)(3)

PE-21 ENVIRONMENTAL CONTROL TRAINING

Control: Ensure employees are provided with initial and periodic training in the operation of environmental controls.

Supplemental Guidance: Examples of environmental controls include but are not limited to fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors and temperature/humidity, HVAC, power, within the facility.

Control Enhancements: None.

LOW Not Required	**MOD** PE-21	**HIGH** PE-21

FAMILY: PLANNING CLASS: MANAGEMENT

Each information system must be subjected to a C&A process and accredited (authorized) prior to being allowed to process NNSA/DOE information. This measure ensures that all the cyber security measures have been implemented and operate as specified. This measure supports all the principles.

Planning				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1
PL-2	Information System Security Plan	PL-2	PL-2	PL-2
PL-3	Information System Security Plan Update	PL-3	PL-3	PL-3
PL-4	Rules of Behavior	PL-4	PL-4	PL-4
PL-5	Privacy Impact Assessment	PL-5	PL-5	PL-5
PL-6	Security Related Activity Planning	PL-6	PL-6	PL-6

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Control: Develop, disseminate, and periodically review/update:

a. A formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

Supplemental Guidance: The security planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required.

Control Enhancements: None.

LOW PL-1	**MOD** PL-1	**HIGH** PL-1

PL-2 INFORMATION SYSTEM SECURITY PLAN

Control: Develop and implement a security plan for each information system and application that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Components shared by one or more system must also be addressed in the ISSP, tested, and risk assessed. Designated officials within the organization review, and the DAA approves the plan.

Supplemental Guidance: The security plan is aligned with the organization's information system architecture and information security architecture.

LOW PL-2	**MOD** PL-2	**HIGH** PL-2

PL-3 SYSTEM SECURITY PLAN UPDATE

Control: Define and document procedures to require a review of each ISSP at least annually and to revise the plan to address significant changes or problems identified during plan implementation or security control assessments.

Supplemental Guidance: Significant changes are defined in advance by the organization and identified in the configuration management process.

Control Enhancements: None.

LOW PL-3	**MOD** PL-3	**HIGH** PL-3

PL-4 RULES OF BEHAVIOR

Control: Establish and make readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, including consent to monitoring, before authorizing access to the information system and its resident information.

Supplemental Guidance: Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy.

Control Enhancements: None.

LOW PL-4	**MOD** PL-4	**HIGH** PL-4

PL-5 PRIVACY IMPACT ASSESSMENT

Control: Conduct a privacy impact assessment on external-facing information systems that contain privacy information.

Supplemental Guidance: OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002.

Control Enhancements: None.

LOW PL-5	**MOD** PL-5	**HIGH** PL-5

PL-6 SECURITY-RELATED ACTIVITY PLANNING

Control: Plan and coordinate security-related activities (e.g., security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises) affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

Supplemental Guidance: Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.

Control Enhancements: None.

LOW PL-6	**MOD** PL-6	**HIGH** PL-6

FAMILY: PERSONNEL SECURITY CLASS: OPERATIONAL

Effective administration of users' computer access is essential to maintaining system security. Administration of system users focuses on identification, authentication, and access authorizations. NNSA requires that each operating unit implement and maintain a process of auditing and otherwise periodically verifying the legitimacy of current accounts and access authorizations. In addition, they are to address the timely modification or removal of access and associated issues for employees who are reassigned, promoted, or terminated. Many important issues in computer security involve Federal and contractor system users, designers/programmers, implementers/maintainers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their job. No computer system can be secured without properly addressing these security issues.

Personnel Security				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1
PS-2	Position Categorization	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3 (1) PS-3	PS-3 (1) PS-3	PS-3 (1) PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4
PS-5	Personnel Transfer	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6 (1)	PS-6 (1)(2)	PS-6 (1)(2)
PS-7	Third-Party Personnel Security	PS-7	PS-7 (1)	PS-7 (1)
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control: Ensure the following is developed, disseminated, and periodically reviewed/updated:

a. A formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Supplemental Guidance: The personnel security policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general, and for a particular information system, when required.

Control Enhancements: None.

LOW PS-1	**MOD** PS-1	**HIGH** PS-1

PS-2 POSITION CATEGORIZATION

Control: Ensure that all cyber security roles are designated as high, medium, or low risk and screening criteria is established. The roles are reviewed and categorized for their potential adverse impact on the efficiency and integrity of the system, at least every three years.

Supplemental Guidance: This control is intended to ensure that all positions within an NNSA Element have been assessed for screening requirements. For instance, some positions are "coded" as requiring minimum clearance levels.

Control Enhancements: None. See PS-3 for additional information.

LOW PS-2	**MOD** PS-2	**HIGH** PS-2

PS-3 PERSONNEL SCREENING

Control: Ensure all personnel are subjected to an appropriate screening process prior to permitting permanent access to information and information system resources. Screening must be performed for NNSA Element employees, contractors, and any "guests" prior to their being given access to the Element's systems and networks. A risk-based, cost-effective approach must be followed to determine the risk of harm to the system in comparison to the opportunity for personnel performing the following functions:

- Personnel with cyber security authority, "root" access to systems, or access to software source code who have opportunity to bypass system security control settings – for example, network/system administrator, system developer, and cyber security program positions (such as ISSOs and ISSMs).

- User with root access to information systems who may modify core data stores, users with authority to electronically approve financial transactions, or users with access to personal/Privacy Act/other protected data (e.g., social security numbers in human resource systems) other than their own.

- Users with access to an NNSA Element's local area network, e-mail, basic office applications (such as Microsoft Office or Corel Office suites), and personal data records (i.e., only personal/private information pertaining to themselves such as their personal time and attendance record or Thrift Savings Plan account).

  Supplemental Guidance: Screening is consistent with organizational policy, regulations, and guidance.

Control Enhancements:

(1) Every user who has access to a system processing classified information must be cleared and indoctrinated for that classified information.

(2) The User must follow the policies and procedure of the User Control Group.

LOW	PS-3	**MOD**	PS-3 (1)	**HIGH**	PS-3 (1)
LOW	PS-3	**MOD**	PS-3	**HIGH**	PS-3

PS-4 PERSONNEL TERMINATION

Control: Upon termination of individual employment, ensure information system access is terminated, exit interviews are conducted, and ensure there are procedures for the return of all organizational information system-related property. Ensure appropriate personnel are provided with access to official records created by the terminated employee that are stored on organizational information systems, before the systems are recycled or disposed.

Supplemental Guidance: Information system-related property includes, for example, keys, identification cards, access tokens, and building passes. Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Control Enhancements: None.

LOW PS-4	**MOD** PS-4	**HIGH** PS-4

PS-5 PERSONNEL TRANSFER

Control: Ensure information systems/facilities access authorizations are reviewed when personnel are reassigned or transferred to other positions within the organization and appropriate actions are initiated.

Supplemental Guidance: Appropriate actions that may be required include: (i) returning old and issuing new keys, identification cards, building passes; (ii) closing old accounts and establishing new accounts; (iii) changing system access authorizations; and (iv) providing for access to official records created or controlled by the employee at the old work location and in the old accounts. A change in user access and, therefore, suitability and risk may arise when an individual changes job duties within an NNSA Element or changes Elements.

Control Enhancements: None.

LOW PS-5	**MOD** PS-5	**HIGH** PS-5

PS-6 ACCESS AGREEMENTS

Control: Complete appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access.

Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements.

Control Enhancements:

(1) The organization ensures that access to information with special protection measures (e.g., privacy or proprietary information) is granted only to individuals who:

(a) Have a valid need-to-know that is demonstrated by assigned official government duties, and

(b) Satisfy associated personnel security criteria (e.g., position sensitivity background screening requirements).

(2) The NNSA Element ensures that access to classified information with special protection measures (e.g., SAP) are granted only to individuals who:

(a) Have a valid need-to-know that is demonstrated by assigned official government duties, and

(b) Satisfy associated personnel security criteria, and

(c) Read, understand and signed a non-disclosure agreement.

LOW PS-6 (1)	**MOD** PS-6 (1)(2)	**HIGH** PS-6 (1)(2)

PS-7 THIRD-PARTY PERSONNEL SECURITY

Control: Comply with personnel security requirements including security roles and responsibilities for third-party providers (e.g., contractors and other organizations providing information system development, information technology services, outsourced applications, and network and security management) and monitor provider compliance to ensure adequate security.

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents.

Control Enhancement:

(1) The organization explicitly defines government oversight and end-user roles and responsibilities relative to third-party provided services.

LOW PS-7	**MOD** PS-7 (1)	**HIGH** PS-7 (1)

PS-8 PERSONNEL SANCTIONS

Control: Comply with the formal sanctions process for personnel failing to comply with established information security policies and procedures.

Supplemental Guidance: The sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The sanctions process can be included as part of the general personnel policies and procedures for the organization.

Control Enhancements: None.

LOW PS-8	**MOD** PS-8	**HIGH** PS-8

FAMILY: RISK ASSESSMENT CLASS: MANAGEMENT

Risk measures the combined results of threat likelihood of occurrence and level of impact on NNSA Element operations (including mission, functions, credibility, or reputation), Agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. Risk management is the ongoing process of managing risks to Agency operations (including mission, functions, image, or reputation), NNSA assets, or individuals resulting from the operation of an information system. It includes risk assessment; the selection, implementation, and assessment of cost-effective security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, Directives, policies, or regulations.

A system owner, in consultation with the Information System Security Officer and other interested parties, such as the Designated Approving Authority, uses the results of this evaluation to determine countermeasures to prevent or mitigate risk. The Information System Security Officer can assist by providing the system owner with a risk assessment methodology and by providing assistance in interpreting the risk assessment results and suggesting possible cost-effective security countermeasure alternatives.

Risk Assessment				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3
RA-4	Risk Assessment Update	RA-4	RA-4	RA-4
RA-5	Vulnerability Scanning	RA-5 (1)(2)(3)	RA-5 (1)(2)(3)	RA-5 (1)(2)(3)

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: Develop, disseminate, and periodically review/update:

a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Supplemental Guidance: Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required.

Control Enhancements: None.

LOW RA-1	**MOD** RA-1	**HIGH** RA-1

RA-2 SECURITY CATEGORIZATION

Control: The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the system security plan. Designated management officials within the organization review and approve the security categorizations.

Supplemental Guidance: The organization conducts risk assessments and security categorizations as an organization-wide activity. The organization also considers potential impacts to other organizations, both locally and through interconnections, and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system, re-assesses the risks and adjusts the controls accordingly. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk. Related security controls: MP-4 and SC-7.

Control Enhancements: None.

LOW RA-2	**MOD** RA-2	**HIGH** RA-2

RA-3 RISK ASSESSMENT

Control: Conduct assessments of 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 the operations and assets of the NNSA Element.

Supplemental Guidance: Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to

organizational operations, organizational assets, or individuals based on the operation of the information system. The organization also considers potential impacts to other organizations both locally and through interconnections, and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system, re-assesses the risks and adjusts the controls accordingly. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities).

Control Enhancements: None.

LOW RA-3	**MOD** RA-3	**HIGH** RA-3

RA-4 RISK ASSESSMENT UPDATE

Control: Update the risk assessment at least every three years or whenever there are security significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.

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.

Supplemental Guidance: None.

Control Enhancements: None.

LOW RA-4	**MOD** RA-4	**HIGH** RA-4

RA-5 VULNERABILITY SCANNING

Control:

a. Scan for vulnerabilities in the information system at least quarterly or when significant new vulnerabilities potentially affecting the system/enterprise are identified and reported.

b. The information obtained from the vulnerability scanning process is shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems.

Supplemental Guidance: Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. Note: Vulnerability information concerning a specific classified system must be appropriately protected, and communicated through secure means if the affected system may be exploited.

Control Enhancements:

(1) The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.

(2) The organization updates the list of information system vulnerabilities scanned when significant new vulnerabilities are identified and reported.

(3) The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of scan coverage, including vulnerabilities checked and information system components scanned.

LOW RA-5 (1)(2)(3)	**MOD** RA-5 (1)(2)(3)	**HIGH** RA-5 (1)(2)(3)

FAMILY: SYSTEM AND SERVICES ACQUISITION CLASS: MANAGEMENT

System and Services Acquisition				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**

System and Services Acquisition				
Control Number	Control Name	Control Baselines		
		Low	Moderate	High
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	Life Cycle Support	SA-3	SA-3	SA-3
SA-4	Acquisitions	SA-4	SA-4 (1)	SA-4 (1)
SA-5	Information System Documentation	SA-5	SA-5 (1)(2)	SA-5 (1)(2)(3)
SA-6	Software Usage Restrictions	SA-6 (1)(2)	SA-6 (1)(2)	SA-6 (1)(2)
SA-7	User Installed Software	SA-7	SA-7	SA-7
SA-8	Security Design Principles	Not Required	SA-8	SA-8
SA-9	Outsourced Information System Services	SA-9	SA-9	SA-9 (1)
SA-10	Developer Configuration Management	Not Required	SA-10	SA-10 (1)
SA-11	Developer Security Testing	Not Required	SA-11 (1)	SA-11 (1)

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control: Develop, disseminate, and periodically review/update:

a. A formal, documented, system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

Supplemental Guidance: The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general, and for a particular information system, when required.

Control Enhancements: None.

LOW SA-1	**MOD** SA-1	**HIGH** SA-1

SA-2 ALLOCATION OF RESOURCES

Control: Determine, document, and allocate as part of the capital planning and investment control process, the resources required to adequately protect the information system. The organization includes the determination of security requirements for the information system in mission/business case planning and establishes a discrete line item for information system security in the organization's programming and budgeting documentation. Allocations must be based on a risk management assessment.

Supplemental Guidance: None

Control Enhancements: None.

LOW SA-2	**MOD** SA-2	**HIGH** SA-2

SA-3 LIFE CYCLE SUPPORT

Control: Manage information systems using a system development life cycle methodology that includes information security considerations.

Supplemental Guidance: None.

Control Enhancements: None.

LOW SA-3	**MOD** SA-3	**HIGH** SA-3

SA-4 ACQUISITIONS

Control: Include security requirements and/or security specifications, either explicitly or by reference, in information system and information technology service acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Guidance: When security requirements are articulated by reference, the reference needs to be specific regarding which control is assigned.

Control Enhancements:

(1) The organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

LOW SA-4	**MOD** SA-4 (1)	**HIGH** SA-4 (1)

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control: Obtain, protect as required, and make available to authorized personnel, adequate documentation for each information system. Provides compensating security controls, if needed, when adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer).

Supplemental Guidance: None.

Control Enhancements:

(1) User guide that describes:

(a) Information on effectively using the system's security features,

(b) Methods for user interaction with the system, which enables the users to use the information system in a secure manner,

(c) User accessible security functions and effective use, and

(d) User's role in maintaining the security of the information.

(2) Administrator guide that describes:

(a) Secure configuration, installation, and operation of the information system; and

(b) Effective use and maintenance of the system’s security features.

(c) Responsibilities of administrators on what they can/cannot do.

(3) System/manufacturer documentation that describes:

(a) The functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls, and to verify the integrity of the system.

(b) The design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

(c) The high and low-level design of the information system in terms of modules with each subsystem and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among the modules).

(d) The information system external interfaces with sufficient detail to permit analysis and testing of the controls.

LOW SA-5	**MOD** SA-5 (1)(2)	**HIGH** SA-5 (1)(2)(3)

SA-6 SOFTWARE USAGE RESTRICTIONS

Control: Comply with software usage restrictions (e.g., contract agreements and copyright restrictions) and other restrictions as established in the NNSA PCSP.

Supplemental Guidance: Software and associated documentation are used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to controls copying and distribution.

Control Enhancement:

(1) The organization ensures that binary or machine executable code without accompanying source code from the public domain or from sources with limited or no vendor maintenance such as those commonly known as freeware or shareware are not used in the information system unless they are necessary for mission accomplishment and there are no alternative IT solutions available.

(2) The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

LOW SA-6 (1)(2)	**MOD** SA-6 (1)(2)	**HIGH** SA-6 (1)(2)

SA-7 USER INSTALLED SOFTWARE

Control: Enforce explicit rules governing the installation of external software (e.g., personally owned software and public domain software) by users.

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software that is free only for personal, not government use, and software whose pedigree with regard to being potentially malicious is unknown or suspect).

Control Enhancements: None.

LOW SA-7	**MOD** SA-7	**HIGH** SA-7

SA-8 SECURITY ENGINEERING PRINCIPLES

Control: Design and implement the information system using security engineering principles.

Supplemental Guidance: Examples of engineering principles for information systems include but are not limited to: layered protections, establish sound security policy and controls as the foundation for design, treat security as an integral part of the system development life-cycle, delineate physical and logical security boundaries, ensure developers are trained on how to develop secure software for systems, tailor security controls to meet organizational and operational needs, reduce risk to acceptable levels, thus enabling risk executives to make informed decisions. The application of security engineering principles are primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.

Control Enhancements: None.

LOW Not Required	**MOD** SA-8	**HIGH** SA-8

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Control: Ensure that third-party providers of information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements. Each NNSA Element is required to monitor security control compliance for outsourced services.

Supplemental Guidance: An external information system service is a service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. Ultimately, the responsibility for adequately mitigating risks to the organization's operations and assets, and to individuals, arising from the use of external information system services remains with the authorizing official. Authorizing officials must require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk to its operations and assets, or to individuals. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.

Control Enhancement:

(1) The organization ensures that the acquisition or outsourcing of dedicated IA services such as incident monitoring, analysis and response; operation of IA devices such as firewalls; or key management services are supported by a formal risk analysis and approved by site management.

LOW SA-9	**MOD** SA-9	**HIGH** SA-9 (1)

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Control: Ensure that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.

Supplemental Guidance: None.

Control Enhancement:

(1) The organization ensures that information system developers provide an integrity check of the information software that allows the organization to verify the integrity of software after delivery.

LOW Not Required	**MOD** SA-10	**HIGH** SA-10 (1)

SA-11 DEVELOPER SECURITY TESTING

Control: Create a security test and evaluation plan, implement the plan, and document the results.

Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security C&A process for the delivered information system. Related security controls: CA-2 and CA-4.

Control Enhancements:

(1) The organization requires the information system developers to perform a vulnerability analysis, to document the identified vulnerabilities, and explain why each identified vulnerability cannot be exploited in the intended environment.

LOW Not Required	**MOD** SA-11 (1)	**HIGH** SA-11 (1)

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS: TECHNICAL**

System and Communications Protection				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1 (1)	SC-1 (1)
SC-2	Application Partitioning	Not Required	SC-2	SC-2

System and Communications Protection				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
SC-3	Security Function Isolation	SC-3	SC-3	SC-3 (1)(2)(3)(4)(5)
SC-4	Information Remnants	Not Required	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5 (1)(2)	SC-5 (1)(2)	SC-5 (1)(2)(3)
SC-6	Resource Priority	Not Required	SC-6	SC-6
SC-7	Boundary Protection	SC-7 (1)(2)(3)(4)(5)(6)	SC-7 (1)(2)(3)(4)(5)(6)(7)	SC-7 (1)(2)(3)(4)(5)(6)(7)
SC-8	Transmission Integrity	SC-8	SC-8 (1)(2)	SC-8 (1)(2)
SC-9	Transmission Confidentiality	SC-9 (1)(2)(4)	SC-9 (1)(2)(3)(4)(5)	SC-9 (1)(2)(3)(4)(5)
SC-10	Network Disconnect	SC-10	SC-10	SC-10
SC-11	Trusted Path	Not Required	Not Required	Not Required
SC-12	Cryptographic Key Establishment and Management	SC-12 (2)	SC-12 (1) and (2) or (3)	SC-12 (1) and (2) or (3)
SC-13	Use of Validated Cryptography	SC-13	SC-13	SC-13
SC-14	Public Access Protections	SC-14	SC-14	Not Required
SC-15	Collaborative Computing	SC-15 (1)(2)(3)	SC-15 (1)(2)(3)	SC-15 (1)(2)(3)
SC-16	Transmission of Security Parameters	Not Required	Not Required	Not Required
SC-17	Public Key Infrastructure Certificates	Not Required	SC-17	SC-17

System and Communications Protection				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
SC-18	Mobile Code	Not Required	SC-18	SC-18
SC-19	Voice Over Internet Protocol	SC-19	SC-19	SC-19
SC-20	Secure Name/Address Resolution Service (Authentication Source)	Not Required	SC-20 (1)	SC-20 (1)
		Not Required	Not Required	SC-20
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolve)	Not Required	Not Required	SC-21 (1)
		Not Required	Not Required	SC-21
SC-22	Architecture and Provisioning for Name Address Resolution Service	Not Required	SC-22	SC-22
SC-23	Session Authenticity	Not Required	SC-23	SC-23

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control: Develop, disseminate, and periodically review/update:

a. A formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

Supplemental Guidance: The system and communications protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies,

regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required.

Control Enhancement:

(1) The communications links connecting the components of the systems, associated data communications, and networks shall be protected in accordance with Departmental policies and procedures applicable to the sensitivity level of the data being transmitted.

LOW SC-1	**MOD** SC-1 (1)	**HIGH** SC-1 (1)

SC-2 APPLICATION PARTITIONING

Control: The information system separates user functionality (including user interface services) from information system management functionality.

Supplemental Guidance: The information system physically or logically separates user interface services (e.g., public Web pages) from information storage and management services (e.g., data base management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate

Control Enhancements: None.

LOW Not Required	**MOD** SC-2	**HIGH** SC-2

SC-3 SECURITY FUNCTION ISOLATION

Control:

a. The information system isolates security functions from non-security functions by means of partitions, domains, including control of access to and integrity of, the hardware, software, and firmware that performs the security functions.

b. The information system must maintain a separate execution domain (e.g., address space) for each executing process.

Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of partitions, domains, including control of access to and integrity of, the hardware, software, and firmware that perform those security functions.

Control Enhancements:

(1) The information system employs underlying hardware separation mechanisms to facilitate security function isolation.

(2) The information system isolates critical security functions (i.e., functions enforcing access and information flow control) from both nonsecurity functions and from other security functions.

(3) The information system minimizes the number of nonsecurity functions included within the isolation boundary containing security functions

(4) The information system security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.

(5) The information system security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

LOW SC-3	**MOD** SC-3	**HIGH** SC-3(1)(2)(3)(4)(5)

SC-4 INFORMATION REMNANCE

Control: Prevent unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: Control of information system remnance, sometimes referred to as object reuse, or data remnance, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.

Control Enhancements: None.

LOW Not Required	**MOD** SC-4	**HIGH** SC-4

SC-5 DENIAL OF SERVICE PROTECTION

Control: Protect against or limit the effects of the types of denial of service attacks listed in the information system ISSP.

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy.

Control Enhancements:

(1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.

(2) The information system manages excess capacity to limit the effects of information flooding types of denial of service attacks.

(3) The information system fails securely.

LOW SC-5 (1)(2)	**MOD** SC-5 (1)(2)	**HIGH** SC-5 (1)(2)(3)

SC-6 RESOURCE PRIORITY

Control: Limit the use of resources by priority.

Supplemental Guidance: Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process.

Control Enhancements: None.

LOW Not Required	**MOD** SC-6	**HIGH** SC-6

SC-7 BOUNDARY PROTECTION

Control:

a. Monitor and control communications at the accreditation boundary of the information system, and at key internal boundaries within the system.

b. Connections to external networks or information system occur through managed interfaces consisting of appropriate boundary protection devices arranged in an effective architecture.

Supplemental Guidance: Boundary protection devices can consist of proxies, gateways, routers, firewalls, guards, and encrypted tunnels. An effective approach for accomplishing this from an architectural standpoint is by using routers protecting firewalls and application gateways residing on a protected sub network commonly referred to as a demilitarized zone (DMZ).

As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. Risk and security categorization guides the selection of appropriate candidates for domain partitioning.

The organization carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related security controls: MP-4 and RA-2.

Control Enhancements:

(1) The organization physically allocates publicly accessible information system components to separate sub networks with separate, physical network interfaces.

(2) The organization prevents public access into the organization's internal networks except as appropriately mediated.

(3) The organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.

(4) The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.

(5) The information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).

(6) The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the

information system boundary when there is an operational failure of the boundary protection mechanisms.

(7) The organization ensures that classified information systems do not directly connect to or allow any Internet access without NSA Need to Know (NTK), or an approved controlled interface, and connections where across/through networks where people are not cleared – RD 'Q, clearance and 'NSI 'l'clearance.

LOW	SC-7 (1)(2)(3)(4)(5)(6)	**MOD**	SC-7 (1)(2)(3)(4)(5)(6)(7)	**HIGH**	SC-7 (1)(2)(3)(4)(5)(6)(7)

SC-8 TRANSMISSION INTEGRITY

Control: Protect the integrity of transmitted information.

Supplemental Guidance: If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk.

Control Enhancements:

(1) The organization employs mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

(2) Information systems transmitting classified information will use NSA-approved NTK mechanisms commensurate for the classification and sensitivity of the information.

LOW	SC-8	**MOD**	SC-8 (1)(2)	**HIGH**	SC-8 (1)(2)

SC-9 TRANSMISSION CONFIDENTIALITY

Control: Protect the confidentiality of transmitted information.

Supplemental Guidance: If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related security control: AC-17.

Control Enhancements (***To be used as appropriate***):

(1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.

Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems.

(2) The information system uses FIPS-validated cryptography to encrypt controlled unclassified data to prevent unauthorized disclosure of information during transmission. See Chapter VII for special considerations for Sensitive Unclassified Information.

Enhancement Supplemental Guidance: This control is typically applied where the communications infrastructure falls outside of organizational control.

(3) The information system uses NSA-approved cryptography to separately encrypt classified data transmitted through a network that is accredited to a lower level than the data being transmitted.

(4) The information system uses, at a minimum, FIPS-validated cryptography to encrypt information in transit through a network at the same classification level that must be separated for need-to-know or formal access reasons.

(5) Information systems transmitting classified information will use NSA-approved encryption-1 mechanisms commensurate for the classification and sensitivity of the information.

LOW SC-9 (1)(2)(4)	**MOD** SC-9 (1)(2)(3)(4)(5)	**HIGH** SC-9 (1)(2)(3)(4)(5)

SC-10 NETWORK DISCONNECT

Control: Terminate a network connection at the end of a session or after a period of inactivity specified in the system's ISSP.

Supplemental Guidance: The organization applies this control within the context of risk management that considers specific mission or operational requirements. Sessions internal to an information system and not initiated externally (i.e., by an external user or external process) can remain active if necessary for the functional capability of the information system.

Control Enhancements: None.

LOW SC-10	**MOD** SC-10	**HIGH** SC-10

SC-11 TRUSTED PATH

Control: NNSA Elements may specify or system owners may elect at their discretion to ensure that information systems establish a trusted path between the user and the security functionality of the system.

Supplemental Guidance: A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).

Control Enhancements: None.

LOW Not Required	**MOD** Not Required	**HIGH** Not Required

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: The organization establishes and manages cryptographic keys using manual procedures or automated mechanisms with supporting procedures.

Supplemental Guidance: This control only applies when cryptography is required and employed within the information system.

Control Enhancements:

(1) The organization implements effective cryptographic key management in support of encryption and provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.

(2) Symmetric Keys are produced, controlled and distributed using NIST-approved key management technology and processes.

Enhancement Supplemental Guidance: Asymmetric keys are produced, controlled and distributed using approved PKI Class 3 certificates or preplaced keying material.

(3) Symmetric Keys are produced, controlled and distributed using NSA-approved key management technology and processes.

Enhancement Supplemental Guidance: Asymmetric keys are produced, controlled and distributed using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.

(4) Symmetric and asymmetric keys are produced, controlled and distributed using NSA-approved key management technology and processes.

LOW SC-12 (2)	**MOD** SC-12 (1) and (2) or (3)	**HIGH** SC-12 (1) and (2) or (3)

SC-13 USE OF CRYPTOGRAPHY

Control: The information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. See Chapter VII for special considerations for Sensitive Unclassified Information.

Supplemental Guidance: This control only applies when the system is processing, storing or transmitting information requiring cryptographic protection.

Control Enhancement: None.

LOW SC-13	**MOD** SC-13	**HIGH** SC-13

SC-14 PUBLIC ACCESS PROTECTIONS

Control: The information system protects the integrity and availability of publicly available information and applications.

Supplemental Guidance: None.

Control Enhancements: None.

LOW SC-14	**MOD** SC-14	**HIGH** Not Required

SC-15 COLLABORATIVE COMPUTING

Control: Prohibit unauthorized remote activation of collaborative computing mechanisms and provide an explicit indication of use to the local users.

Supplemental Guidance: Collaborative computing mechanisms include, for example, video and audio conferencing capabilities. Explicit indication of use includes, for example, signals to local users when cameras and/or microphones are activated.

Control Enhancements:

(1) The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.

(2) The information system or supporting environment blocks both inbound and outbound traffic between instant messaging (IM) clients that are independently configured by end users and public service providers.

(3) The organization ensures that information systems in secure work areas have cameras and microphone capabilities disabled or removed.

LOW SC-15 (1)(2)(3)	**MOD** SC-15 (1)(2)(3)	**HIGH** SC-15 (1)(2)(3)

SC-16 TRANSMISSION OF SECURITY PARAMETERS

Control: NNSA Elements or system owners may elect, at their discretion, to ensure that information systems reliably associate security parameters (e.g., security labels and markings) with information exchanged between information systems.

Supplemental Guidance: Security parameters include, for example, security labels and markings. Security parameters may be explicitly or implicitly associated with the information contained within the information system.

Control Enhancements: None

LOW Not Required	**MOD** Not Required	**HIGH** Not Required

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: Public key certificates are issued under an appropriate certificate policy or the public key certificates are obtained under an appropriate certificate policy from an approved service provider.

Supplemental Guidance: For user certificates, each agency either establishes an agency certification authority cross-certified with the Federal Bridge Certification Authority at medium assurance or higher or uses certificates from an approved, shared service provider, as required by OMB Memorandum 05-24.

Control Enhancements: None.

LOW Not Required	**MOD** SC-17	**HIGH** SC-17

SC-18 MOBILE CODE

Control:

a. Establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and

b. Document, monitor, and control the use of mobile code within the information system.

Supplemental Guidance: Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition or introduction of unacceptable mobile code within the information system.

Control Enhancements: None

LOW Not Required	**MOD** SC-18	**HIGH** SC-18

SC-19 VOICE OVER INTERNET PROTOCOL

Control:

a. Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and

b. Document, monitor, and control the use of VoIP within the information system.

Supplemental Guidance: None

Control Enhancements: None.

LOW SC-19	**MOD** SC-19	**HIGH** SC-19

SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control: The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.

Supplemental Guidance: This control enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data.

Control Enhancement:

(1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

LOW	Not Required	**MOD**	SC-20 (1)	**HIGH**	SC-20 (1)
LOW	Not Required	**MOD**	Not Required	**HIGH**	SC-20

SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Control: The information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.

Supplemental Guidance: A resolving or caching domain name system (DNS) server is an example of an information system that provides name/address resolution service for local clients and authoritative DNS servers are examples of authoritative sources.

Control Enhancement:

(1) The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service.

LOW	Not Required	**MOD**	Not Required	**HIGH**	SC-21 (1)
LOW	Not Required	**MOD**	Not Required	**HIGH**	SC-21

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

Control: The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.

Supplemental Guidance: A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are

commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). If organizational information technology resources are divided into those resources belonging to internal networks and those resources belonging to external networks, authoritative DNS servers with two roles (internal and external) are established. The DNS server with the internal role provides name/address resolution information pertaining to both internal and external information technology resources while the DNS server with the external role only provides name/address resolution information pertaining to external information technology resources. The list of clients who can access the authoritative DNS server of a particular role is also specified.

Control Enhancements: None.

LOW Not Required	**MOD** SC-22	**HIGH** SC-22

SC-23 SESSION AUTHENTICITY

Control: The information system provides mechanisms to protect the authenticity of communications sessions.

Supplemental Guidance: This control focuses on communications protection at the session, versus packet, level. The intent of this control is to implement session-level protection where needed (e.g., in service-oriented architectures providing Web-based services).

Control Enhancements: None.

LOW Not Required	**MOD** SC-23	**HIGH** SC-23

FAMILY: SYSTEM AND INFORMATION INTEGRITY CLASS: OPERATIONAL

Integrity controls protect data in an information system from accidental or malicious alteration or destruction and provide assurance to the user that the information meets criteria about its quality and reliability.

System and Information Integrity				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1

System and Information Integrity				
Control Number	**Control Name**	**Control Baselines**		
		Low	**Moderate**	**High**
SI-2	Flaw Remediation	SI-2	SI-2(1)(2)	SI-2 (1)(2)
SI-3	Malicious Code Protection	SI-3 (1)(3)	SI-3 (1)(2)(3)(4)(5)	SI-3 (1)(2)(3)(4)(5)
SI-4	Information System Monitoring Tools and Techniques	SI-4	SI-4(1)	SI-4 (1)(2)(3)
SI-5	Security Alerts and Advisories	SI-5	SI-5	SI-5 (1)
SI-6	Security Functionality Verification	SI-6	SI-6	SI-6 (1)
SI-7	Software and Information Integrity	Not Required	SI-7 (1)	SI-7 (1)
SI-8	Spam and Spyware Protection	SI-8 (1)	SI-8 (1)(2)(3)(4)	SI-8 (1)(2)(3)(4)
SI-9	Information Input Restrictions	SI-9	SI-9	SI-9
SI-10	Information Input Accuracy, Completeness, and Validity	Not Required	SI-10	SI-10
SI-11	Error Handling	SI-11	SI-11	SI-11
SI-12	Information Output Handling and Retention	SI-12	SI-12	SI-12

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control: Develop, disseminate, and periodically review/update:

a. A formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

Supplemental Guidance: The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required.

Control Enhancements: None.

LOW SI-1	**MOD** SI-1	**HIGH** SI-1

SI-2 FLAW REMEDIATION

Control: Identify, report, and correct information system flaws and share information on identified flaws with the NNSA Information Assurance Response Center.

Supplemental Guidance: It is important for the organization to identify information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) should consider promptly installing newly released security relevant patches, service packs, and hot fixes. It is **strongly** recommended that the organization test software flaw remediation fixes (e.g., patches, service packs, and hot fixes) for effectiveness and potential side effects on the organization's information systems prior to installation. Flaws discovered during security assessments, continuous monitoring, and incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation is incorporated into configuration management as an emergency change. Related security controls: CA-1, CA-4, CA-7, CM-3, IR-4, and SI-11.

Control Enhancements:

(1) The organization centrally manages the flaw remediation process and installs updates manually or automatically.

Enhancement Supplemental Guidance: Due to the system integrity and availability concerns organizations should give careful consideration to the methodology in complying with this requirement.

(2) The organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.

LOW SI-2 (1)	**MOD** SI-2 (1)(2)	**HIGH** SI-2 (1)(2)

SI-3 MALICIOUS CODE PROTECTION

Control: Employ, implement and maintain malicious code protection on each information system.

Supplemental Guidance: At a minimum the organization should consider malicious code protection mechanisms at critical information system entry and exit points. Examples of entry and exit points are firewalls, mail servers, SMTP gateways, Web servers, proxy servers and remote access servers. The organization should consider using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and

servers and another vendor for workstations). The organization should also consider the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Control Enhancements:

(1) The organization centrally manages malicious code protection mechanisms.

(2) The information system automatically updates malicious code protection mechanisms.

(3) The organization updates malicious code protection mechanisms to include the latest virus and spyware definitions when new releases are available, in accordance with organizational configuration management policy and procedures.

(4) The organization employs, implements, and maintains malicious code protection countermeasures on mobile computing devices on the network.

(5) The organization employs, implements and maintains malicious code protection countermeasures to detect and eradicate malicious code transported by electronic mail, electronic mail attachments, Internet accesses and removable media.

LOW SI-3 (1)(3) (4)(5)	**MOD** SI-3 (1)(2)(3)(4)(5)	**HIGH** SI-3 (1)(2)(3)(4)(5)

SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES

Control:

a. Employ tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system. Refer to INFOCON in NAP 14.1-C.

b. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

c. Require Internet access points to have network-based intrusion detection systems and require all Internet-accessible servers to have host-based intrusion detection systems in place and functioning.

Supplemental Guidance: Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect

essential information. Monitoring devise are also deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices are used to track the impact of security changes to the information system. The granularity of the information collected is determined by the organization based upon its monitoring objectives and the capability of the information system to support such activities.

Control Enhancements:

(1) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

(2) The information system provides a real-time alert when the following indications of compromise or potential compromise occur: [*organization-defined list of compromise indicators*].

NNSA also recommends the following:

- Networking individual intrusion detection tools into a system-wide intrusion detection system using common protocols.
- Employing automated tools to support near-real-time analysis of events in support of detecting system-level attacks.
- Employing automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

(3) The information system notifies the appropriate security personnel of suspicious events and takes the least disruptive action to terminate suspicious events.

LOW SI-4 (1)	**MOD** SI-4 (1)(2)	**HIGH** SI-4 (1)(2)(3)

SI-5 SECURITY ALERTS AND ADVISORIES

Control: Receive information system security alerts/advisories on a regular basis, issue alerts/advisories to appropriate personnel, and takes appropriate actions in response. The organization documents the types of actions to be taken in response to security alerts/advisories and validates that the action was performed correctly.

Supplemental Guidance: The organization should also maintain contact with special interest groups (e.g., information security forums) that: (i) facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies); (ii)

provide access to advice from security professionals; and (iii) improve knowledge of security best practices.

Control Enhancement:

(1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

LOW SI-5 (1)	**MOD** SI-5 (1)	**HIGH** SI-5 (1)

SI-6 SECURITY FUNCTIONALITY VERIFICATION

Control: Document security functionality controls, and verify the correct operation of security functions either upon system startup and restart, upon command by user with appropriate privilege, or periodically every quarter and either notify system administrator, shut the system down, or restart the system when anomalies are discovered.

Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required.

Control Enhancements:

(1) The organization employs automated mechanisms to provide notification of failed automated security tests.

(2) The organization employs automated mechanisms to support management of distributed security testing.

LOW Not Required	**MOD** SI-6	**HIGH** SI-6 (1)

SI-7 SOFTWARE AND INFORMATION INTEGRITY

Control: The information system detects and protects against unauthorized changes to software and information.

Supplemental Guidance: The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, and cryptographic hashes) and uses tools to automatically monitor the integrity of the information systems and the applications it hosts.

Control Enhancements:

(1) The NNSA Element provides notification to appropriate individuals upon discovering discrepancies during integrity verification.

(2) The organization employs centrally managed integrity verification tools.

LOW (1)	**MOD** SI-7 (1)	**HIGH** SI-7 (1)

SI-8 SPAM PROTECTION

Control: Employ, implement and maintain spam protection mechanisms within the information system if the system is vulnerable to these threats. If the system is not affected by these threats, define procedures to ensure that the resistant characteristics are documented in the ISSP.

Supplemental Guidance: At a minimum the organization should consider spam protection mechanisms at critical information system entry and exit points. Examples of entry points firewalls, electronic SMTP gateways, mail servers, and remote access servers. Consideration is given to using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations).

Control Enhancements:

(1) The organization centrally manages spam protection mechanisms.

(2) The organization employs implements and maintains spam protection mechanisms on mobile computing devices on the network.

(3) The organization employs, implements and maintains spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet accesses, or other common means.

(4) The information system updates spam protection mechanisms.

LOW SI-8 (1)	**MOD** SI-8 (1)(2)(3)(4)	**HIGH** SI-8 (1)(2)(3)(4)

SI-9 INFORMATION INPUT RESTRICTIONS

Control: Restrict the capability to input information to the information system to authorized personnel.

Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Control Enhancements: None.

LOW SI-9	**MOD** SI-9	**HIGH** SI-9

SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY

Control: The information system checks information for accuracy, completeness, validity, and authenticity.

Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.

Control Enhancements: None.

LOW Not Required	**MOD** SI-10	**HIGH** SI-10

SI-11 ERROR HANDLING

Control: The information system identifies and handles error conditions in an expeditious manner

Supplemental Guidance: Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Control Enhancement: None.

LOW SI-11	**MOD** SI-11	**HIGH** SI-11

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

Control: Handle and retain output from the information system in accordance with the NNSA Element policy and operational requirements.

Supplemental Guidance: None

Control Enhancements: None.

LOW SI-12	**MOD** SI-12	**HIGH** SI-12

This page left intentionally blank.

CHAPTER V: SECURITY CATEGORY

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*, and CNSS Policy No. _xxx___, "*Security Control Catalog for National Security Systems, Extending [NIST SP] 800-53 to National Security Information and National Security Systems*", note that the security controls applied to a particular information system should be commensurate with the potential impact on organizational operations, organizational assets, or individuals should there be a breach in security due to the loss of data or system confidentiality, integrity, or availability.

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, requires organizations to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values assigned to the respective security objectives are the highest values (i.e., high water mark) from among the security categories that have been determined for each type of information resident on the information systems. The generalized format for expressing the security category of an *information system* is:

Information system security category =

{(confidentiality, ***impact-level***), (integrity, ***impact-level***), (availability, ***impact-level***)},

where the acceptable values for potential impact are low, moderate, or high.

Since the potential impact levels for the confidentiality, integrity, and availability security objectives may not be identical for an information system, the high water mark concept is used to determine the impact level of the information system and select an initial set of security controls from the three baselines defined in Chapter IV. 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 greater than moderate. 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, an initial set of security controls can be selected from the baseline controls detailed in Chapter IV.

NNSA has made refinements to the controls noted in NIST SP 800-53 in the following way:

> NNSA specifications of a control parameter or refinement of a control have been incorporated into the control statement.

This page left intentionally blank.

CHAPTER VI: INFORMATION SYSTEM SECURITY PLAN AND ACCREDITATION PACKAGE

1. REQUIREMENTS. The ISSP is a living document that represents the formal agreement among the DAA, the CSSM, and the system owner. The ISSP is developed in the Definition phase and updated in each phase as the system development progresses and new information becomes available. The ISSP and accreditation decision is supported by other documentation included in the C&A Package, such as Risk Assessments, Security Test and Evaluation Plans and Reports, and Privacy Impact Assessment (if necessary). Note that the ISSP may contain the system residual risks.

   a. Every information system must have an Authority to Operate (accredited) that is supported by the documents in its' C&A Package.

   b. At a minimum, each C&A Package must consist of the documents identified in the following paragraphs. If the NNSA Element requires additional information/ documents, they should be identified in the Element's CSPP.

      (1) Information System Security Plan (ISSP) which includes references to the site Security Risk Assessment, Configuration Management Plan, and Contingency Plan;

      (2) Risk Assessment Report;

      (3) Privacy Impact Assessment (if required);

      (4) Security Test and Evaluation (ST&E) Report; and

      (5) Accreditation Letter.

   c. Except for the ST&E Report and the Accreditation Letter, if the required documents exist as part of other NNSA Element documents, the C&A Package may include a complete reference (including location) to those documents.

   d. The Designated Approving Authority must approve the following documents:

      (1) The ISSP is approved prior to the beginning of the control assessments and updated as the result of deficiencies found during the ST&E process;

      (2) The ST&E Plan is approved prior to the start of the ST&E; and

      (3) Deviations must be approved before an information system can be accredited.

2. INFORMATION SYSTEM SECURITY PLAN. An ISSP must be developed and implemented for all information systems. The ISSP provides the system impact

Agreements. The following is the required high-level format for the ISSP: level, types of information processed, security requirements for the system, and a description of the security controls in place or planned for meeting those requirements. The ISSP provides information necessary to secure an information system throughout its life cycle. The ISSP consists of three major parts: the System Description; the System Component Implementation; and any Interconnect

1. System Description

1.1. Management Information

1.1.1. System Name, Identification, and Organization

1.1.2. System Purpose

1.1.3. Personnel Fulfilling Cyber Security Roles

1.1.4. Information Types and System Categorization

1.2. System Composition

1.2.1. System Functional Description, Components, and External Interfaces (Includes System Diagram)

1.2.2. System Boundary Description (May be shown in system diagram)

1.2.3. Form of Accreditation

1.2.4. Hardware/ Software Inventory

1.3. Physical Security Environment

1.3.1. Security Area

1.4. Threat and Risk Information

1.4.1. Threat Assessment

1.4.2. Identification of threats unique to the system

1.4.3. Risk assessment that identifies any new threats or vulnerabilities

1.4.4. Identification of any deviations unique to the system, and their mitigations

1.5. Operational Environment

1.5.1. Access Authorizations Required

1.5.2. Procedures for Account Authorization

1.6. System Security Requirements

1.6.1. Implementation of Security Controls

1.6.2. Deviations

2. System Component Implementation

2.1. System Component Overview (Each Component)

Appendix1 Interconnection Agreement (Each Interconnection)

1. Management Agreements (MOU)

2. Technical Implementation (ISA)

3. ISSP CONTENTS.

a. System Description. The System Description defines the information system composition in terms of one or more system components that will implement the security controls, the information resident on the system, an overview of the security environment (physical, technical and operational) in which the system will reside, and the identification of any additional controls resulting from the evaluation of the security environment or required by the Information System Owner. The System description must address the following information:

(1) Management Information.

(a) System Name, Identification, and Organization. Provide an overview of the system; its name, identification, and organization responsible for its use.

(b) System Purpose (e.g., machine controller, office desktop, etc),

(c) Personnel Fulfilling Cyber Security Roles. As a minimum the: DAA, Information System Security Site Manager (ISSM); Certification Agent (CA) (Note: The ISSM and CA may be the same individual); Information System Owner; Data Owner/ Steward; and the Information System Security Officer (ISSO) are identified.

(d) Identify all information types that are intended to be on the system and categorize the information system based on the security

objectives (confidentiality, integrity, and availability) of each information type. Utilize Section 3 of Appendix 2 to categorize each information type's confidentiality, integrity, availability objectives in terms of Low, Moderate, or High impact levels. The objective with the highest impact level will be used to categorize the information system and select the set of Minimum Security Controls from Chapter IV. Identify if privacy information is hosted on an externally facing (publicly accessible) system; if so, perform a Privacy Impact Assessment, and adjust planned controls as necessary

(2) System Composition:

(a) Identify the hardware and security-relevant software. At a minimum, the following information is required for major system hardware: nomenclature, model, location, (i.e., building/room, number), and manufacturer.

(b) Identify the accreditation boundary.

(c) Identify the form of accreditation that will be used. If either the Site or Type form of accreditation is used include the procedures for certifying and approving the operation of future instantiations of the system/ system component: these procedures must address: the name of the individual or role that will grant the Approval to Operate; and procedures for testing and documenting the certification and ensuring that the ISSP is updated.

(d) Provide an inventory of the hardware and software that makes up the information system.

(3) Physical Security Environment.

(a) Describe the physical environment (type of protection areas [e.g., Property Protection Area, Limited Area, and a Vault Type Room], physical and visual access controls) in which all system components must reside. Identify any physical threats/ vulnerabilities (include Site unique threats from the CSPP and any system unique physical threats/vulnerabilities) that cannot be mitigated by the Minimum Security Controls. Develop a risk assessment to support any additional security controls needed to mitigate the new threats/ vulnerabilities.

(b) Logical Security Environment. Describe each system component (user workstation, application server, router, switch, etc) and the system component interfaces and connections to networks outside the system boundary (e.g., a drawing showing network

connectivity). Identify other systems with which the system component communicates and the connection rules. A block diagram may be used. Ensure that components shared with other networks are identified, and controls to ensure protection of Need to Know (NTK) boundaries are specified and tested.

(4) Threat and Risk Information

(a) Reference the site cyber risk assessment.

(b) Identify any threats that are unique to the system under consideration. Identify any operational threats (include Site unique threats from the CSPP and any system unique operational threats/vulnerabilities) that cannot be mitigated

(c) Include or reference any risk assessment that identifies new threats or vulnerabilities. Develop a risk assessment to support any additional security controls needed to mitigate the new threats.

(d) Identify any deviations unique to the system under consideration, and state the mitigations for those deviations.

(5) Operational Environment.

(a) Identify the user's required access authorization

(b) Describe the processes used for Need-to-Know control and account authorization.

(6) System Security Requirements.

(a) Select the appropriate minimum security control baseline (low, moderate, or high), then provide a thorough description of how all the minimum security controls in the applicable baseline are being implemented. The description should contain: 1) the security control title; 2) how the security control is being implemented. Identify any controls or practices required by the Information System Owner or Data Owner/ Steward. Develop a risk assessment to support any additional security controls needed to support the practices.

(b) Identify all deviations from the Security Controls, and the mitigations for those deviations

4. IMPLEMENTATION OF SYSTEM SECURITY COMPONENTS. A system component implementation description must be developed and incorporated into the ISSP. Describe

the hardware/ software that provide the system security controls implementation for the system component, including networking interfaces.

5. INTERCONNECTION AGREEMENTS. The Interconnection Agreement describes the management and technical operation between organizations and information systems

   a. Memorandum of Understanding (MOU) – The MOU describes the management agreement between Information System Owners of interconnected information systems. The MOU specifies the security management responsibilities of each Information System Owner for the secure operation of the interconnection and authorizes the interconnection.

   b. ISA - The ISA specifies the technical security implementation of the interconnections of two systems. See Appendix C for a sample ISA.

6. PRIVACY IMPACT ASSESSMENT. Privacy Impact Assessments (PIA) provide an analysis of how Personally Identifiable Information (PII) is handled; evaluate security control compliance with legal, regulatory, and policy requirements; determine risk to the information; and evaluate the controls used to mitigate the risks.

7. SECURITY TEST AND EVALUATION REPORT. A comprehensive report results from the Security Test and Evaluation (ST&E) of all security controls for the information system and any instantiations. The results are used to determine whether the controls in the approved ISSP are implemented and operating as intended and are effective in a particular environment and to identify vulnerabilities in the system after the implementation of controls.

8. ACCREDITATION LETTER. The accreditation letter transmits the DAA accreditation decision.

CHAPTER VII: PROTECTION REQUIREMENTS FOR SENSITIVE UNCLASSIFIED INFORMATION (SUI)

1. INTRODUCTION. This chapter establishes the minimum security criteria and processes for the protection of Sensitive Unclassified Information (SUI) including Personally Identifiable Information (PII). All NNSA Elements must develop, document, and implement policies pertaining 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 include the following criteria:

   a. Use of Encryption. Federal Information Processing Standard (FIPS) 140-2 Level 1 or higher encryption is to be implemented for protection of all SUI on portable/mobile devices and removable media, such as CDROMs or thumb drives containing SUI. All portable/mobile devices and removable media used by Federal employees and all DOE contractors who support systems that contain DOE SUI should have an installed capability to encrypt all such information.

   [Cautionary Note: Cryptographic modules validation certificates issued by the Cryptographic Module Validation Program (including FIPS 140-1, 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until the validation certificate is specifically revoked. The FIPS 140-2 standard also acknowledges the use of cryptography approved by the National Security Agency as an appropriate alternative. Consult FIPS 140-2 for specific guidance.]

   The following steps are to be followed to implement this requirement.

      1. Identify all portable/mobile devices that contain SUI. (Note: All portable/mobile devices are assumed to contain PII unless a designated authorizing Federal management official determines there is no PII on the device. A similar process should be established for reviewing SUI, other than PII, that may be on a device.

      2. Purge SUI from all portable/mobile devices for which its presence is not required. (See NAP 14.1-C).

      3. Install encryption software for all portable/mobile devices that contain SUI or may contain SUI in the future.

      4. Provide user training on the use of the encryption software.

      5. Direct and enforce the use of the encryption software to protect SUI on all portable/mobile devices.

b. Encryption is required for protecting SUI hosted on all portable/mobile devices, and any removable media. Encryption of the entire contents of the hard drive(s) of each desktop computer system/workstation (including laptops) is preferred for protection against data theft or loss and additional defense against cyber attacks.

c. FIPS 140-2 Level 1, or higher, encryption must be applied during the transmission of all SUI unless communications media can provide an equivalent protection as determined by the DAA. NIST-certified FIPS 140-1 encryption may be used until the NIST certification expires.

d. Decryption capabilities or recovery of encryption keys must be available, on request, to law enforcement officials, cyber incident management personnel, and cyber forensics personnel.

3. REMOTE ACCESS.

a. Two-factor authentication must be used for all remote access to SUI, including PII. Note that there is no 2-factor authentication on Blackberries; however, passwords are required.

b. Ensure that a time-out function is in place on all information systems supporting remote access to SUI. The time-out function must require re-authentication of remote users if there is a period of 30 minutes or longer of inactivity on user connections to the system.

4. MANAGEMENT OF PII ON PORTABLE and/or MOBILE DEVICES AND REMOVABLE MEDIA.

a. Establish, document, and implement procedures so that any files containing PII on portable and/or mobile devices or removable media are deleted within 90 days of their creation, or that the approval for continued use of these files is documented.1

b. Document the timely review of PII on portable and/or mobile devices and removable media in accordance with Senior DOE Management procedures.

5. Protection requirements and control procedures for SUI, including PII, are to be included in user training.

---

1 Owners of portable/mobile devices and removable media and their supervisors should be involved in the review on the content of their devices that they use, since they are most familiar with such content. The review should be thoroughly and accurately documented to provide sufficient information to properly determine the disposition of the content of each device.

6. Reporting requirements for cyber security incidents involving PII are described in NAP 14.1-C.

APPENDIX A: ACRONYMS

AA	Approving Authority
C&A	Certification and Accreditation
CFO	Chief Financial Officer
CMPC	Classified Matter Protection and Control
CAN	Computer Network Attack
CNE	Computer Network Exploit
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 Systems 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
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSTISSP	National Security Telecommunications and Information Systems Security

Policy

OMB	Office of Management and Budget
OPSEC	Operations Security
PCSP	Program Cyber Security Plan
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
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 system 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.
Consequences 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 are 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 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. Email 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. Written biographies, such as the ones used in pamphlets of speakers.
14. Alma Mater or degree level in biographies
15. 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, and disk packs.
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.