

Approved: 07-02-10

INFORMATION SECURITY



NATIONAL NUCLEAR SECURITY ADMINISTRATION
Office of Defense Nuclear Security

AVAILABLE ONLINE AT:
<http://www.nnsa.energy.gov>

INITIATED BY:
Office of Defense Nuclear Security

(This Page Intentionally Left Blank)

INFORMATION SECURITY

1. **PURPOSE.** This NNSA Policy prescribes the security requirements and restrictions of the U.S. Department of Energy (DOE) National Nuclear Security Administration (NNSA) for the protection and control of matter required to be classified by Federal statutes and regulations. All information security programs, practices, and procedures developed within NNSA must be consistent with and incorporate the requirements of this Policy along with all national requirements (Atomic Energy Act of 1954, Executive Orders, United States Code (U.S.C.), Code of Federal Regulations (CFR), National Industrial Security Program, etc.).

2. **BACKGROUND.** This NNSA Policy (NAP) was developed using DOE M 470.4-4A, *Information Security Manual*, dated 1-16-09, as a baseline and is tailored to meet the programmatic needs of the NNSA. Section A, Classified Matter Protection and Control (CMPC), Chapters I, II and III were reviewed and revised. This NNSA Policy incorporates national-level requirements and most requirements as set by the Department. When establishing new requirements or deleting requirements, NNSA carefully measured the value of the requirements, perceived or actual threat to the protection and control of classified information based on a risk management approach utilizing the DOE O 470.3B, *Graded Security Protection Policy*, dated 1-16-09, and the costs of implementation. Defense Nuclear Security (DNS) worked closely with the DOE Office of Health, Safety, and Security (DOE/HSS) in developing this NAP. DNS will continue to work closely with the Departmental security policy office, as well as with Departmental inspection and oversight offices, in managing the NNSA security policy program. Some specific changes outlined in this NNSA Policy include:
 - a. The removal of Accountable Classified Removable Electronic Media (ACREM) carefully weighed cost versus benefits and restores conformity with the National Industrial Security Program. The National Industrial Security Program Operating Manual (NISPOM) does not require the accounting of information classified at the Secret level. The consequence for loss or compromise of matter classified at the Secret level as established by Executive Order is that its loss would cause serious damage to national security. This change does not impact established accountability requirements for information classified as Top Secret, North Atlantic Treaty Organization (NATO), etc.

 - b. The term vault-type room (VTR) was replaced with the NISPOM term of closed areas (CAs). This change is due to operational necessity because it may be necessary to construct CAs for storage if General Services Administration (GSA)-approved containers or vaults are deemed unsuitable or impractical. The use of CAs within NNSA provides a level of security consistent with national standards and allows increased flexibility in storage of classified matter. CA requirements are contained in the NNSA *Physical Protection* NAP.

 - c. Classified matter-in-use or “day-lock” procedures were restored into this NNSA Policy and are an acceptable, cost-effective way of protecting classified matter in use during working hours. Day-lock benefits from layers of access control and

security at NNSA Sites, and is a virtually unpredictable configuration for an adversary to predict and exploit. Day-lock is a term used for classified matter-in-use during working hours and should not be confused with storage of classified matter.

NOTE: The requirements in Sections B, C and D were not reviewed and except for minor word changes remain unchanged from the DOE policy as written in DOE M 470.4-4A.

3. CANCELLATIONS.

- a. This NNSA Policy does not cancel any NNSA-issued policy. It does, however, replace DOE M 470.4-4A. "cpf "ku'uweeguqtu. for application to the NNSA's Information Security Program.
- b. Cancellation of a Departmental policy (Policy, Order, Manual, or Notice) or NNSA policy does not, by itself, modify or otherwise affect any contractual obligation to comply with the policy. Canceled policies that are incorporated by reference in a contract remain in effect until the contract is modified to delete the references to the requirements in the canceled policies.

4. APPLICABILITY.

- a. All NNSA Elements. Except for the exclusion in paragraph 4d, this NNSA Policy applies to all NNSA elements. This NNSA Policy automatically applies to NNSA elements created after it is issued.
- b. NNSA Federal Employees. Except for the exclusion in paragraph 4d, this NNSA Policy applies to all NNSA Federal employees. All requirements identified in this NNSA Policy as solely a Federal function are individually identified.
- c. NNSA Contractors. Except for the exclusions in paragraph 4d, this NNSA Policy sets forth requirements that will apply to site/facility management contracts.
 - (1) This NNSA Policy must be included in the site/facility management contracts that involve classified matter or nuclear materials and contain DOE Acquisition Regulation (DEAR) clause 952.204-2, *Security Requirements*.
 - (a) NNSA elements must notify contracting officers of affected site/facility management contracts to incorporate this NNSA Policy into those contracts.
 - (b) Once notified, contracting officers are responsible for incorporating this NNSA Policy into the affected contracts via the laws, regulations, and DOE directives clause of the contracts.

- (c) Requirements identified as solely a Federal function will not be incorporated into contracts.
- (2) A violation of the provisions of this NNSA Policy relating to the safeguarding or security of Restricted Data (RD) or other classified information may result in a civil penalty pursuant to subsection a. of section 234B of the Atomic Energy Act of 1954 (42 U.S.C. 2282b). The procedures for the assessment of civil penalties are set forth in 10 CFR 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*.
- (3) As stated in DEAR clause 970.5204-2, *Laws, Regulations, and DOE Directives*, regardless of the performer of the work, site/facility contractors that have this NNSA Policy incorporated into their contracts are responsible for compliance with this NNSA Policy. Affected site/facility management contractors are responsible for flowing down the requirements of this NNSA Policy to subcontracts at any tier to the extent necessary to ensure compliance with the requirements. In doing so, contractors must not unnecessarily or imprudently flow down requirements to subcontracts. That is, contractors must both ensure that they and their subcontractors comply with the requirements of this NNSA Policy and only incur costs that would be incurred by a prudent person in the conduct of competitive business.
- (4) This NNSA Policy does not automatically apply to other than site/facility management contracts. Application of any of the requirements of this NNSA Policy to other than site/facility management contracts will be communicated as follows:
 - (a) Heads of Field Elements and Headquarters NNSA Elements. Review procurement requests for new non-site/facility management contracts that involve classified matter and contain DEAR clause 952.204-2, *Security Requirements*, and ensure that the requirements of this NNSA Policy are included in those contracts.
 - (b) Contracting Officers. Assist originators of procurement requests who want to incorporate the requirements of this NNSA Policy in new non-site/facility management contracts, as appropriate.
- d. Exclusion. In accordance with the responsibilities and authorities assigned by Executive Order 12344, *Naval Nuclear Propulsion Program*, codified at 50 U.S.C. sections 2406, 2511 and to ensure consistency throughout the joint Navy/DOE organization of the Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee all requirements and practices pertaining to this NNSA Policy for activities under the Director's cognizance, as deemed appropriate.

For NNSA HQ elements which are resident at and serviced through DOE Headquarters, this NAP will not be applicable as the security servicing organization is the DOE Office of Health, Safety, and Security (HSS). NNSA will reevaluate the ability to and will be required to continue to follow all DOE Policy, Orders, and Manuals.

5. AUTHORITIES.

- a. Title XXXII of Public Law 106-65, *National Nuclear Security Administration Act*, as amended, which established a separately organized agency within DOE.
- b. Secretary of Energy Delegation Order No. 00-003.00B to the Under Secretary for Nuclear Security, dated 1-22-10.

6. RESPONSIBILITIES.

- a. Under Secretary for Nuclear Security/Administrator, National Nuclear Security Administration.
 - (1) Has authority over, and is responsible for, all programs and activities of the NNSA. This authority includes, but is not limited to, strategic management, policy development and guidance, program management and direction, administration of contracts, and legal issues.
 - (2) Is responsible for the management and implementation of safeguards and security (S&S) programs administered by NNSA.
- b. NNSA General Counsel. Provides timely review and advice on all legal issues relating to the Information Security Program and the protection of classified matter of the NNSA.
- c. NNSA Contracting Officers.
 - (1) After notification by the appropriate program official, incorporate this NNSA Policy into affected contracts via the laws, regulations, and DOE Directives clauses of the contracts.
 - (2) Assist originators of procurement requests who want to incorporate this NNSA Policy in new non-site/facility management contracts, as appropriate.
- d. Chief, Defense Nuclear Security (DNS).
 - (1) Serves as the NNSA Cognizant Security Authority (NNSA CSA) responsible for the development and implementation of security programs and operations for facilities under the purview of NNSA including physical security, personnel security, materials control and accountability, classified and sensitive information protection, and technical security.

NOTE: This authority may be delegated to subordinate NNSA line managers, and delegation must be documented in the appropriate safeguards and security management plan.

- (2) Oversees the security implementation of NNSA Special Access Programs (SAPs) and provides the NNSA portion of the DOE annual report to Congress.
- (3) Participates in international discussions regarding safeguards policies and procedures.
- (4) Issues direction for and oversees implementation of security conditions for operations under the cognizance of the NNSA.
- (5) Establishes a system of control measures to ensure that access to classified matter is limited to authorized persons. These control measures must be appropriate to the environment in which the access occurs and the nature of the matter. The system must include technical, physical, and personnel control measures.
- (6) Develops and allocates the NNSA security budget including budgets for the infrastructure that supports DNS missions.
- (7) Acts as the DOE representative for international S&S policy development including development of guidelines and technical documents and providing technical assistance.
- (8) Develops, manages, and maintains the NATO security policy for DOE.

e. NNSA Site Managers.

- (1) Implement the Information Security Program as the NNSA CSA for their specific site.
- (2) Re-delegate authorities as necessary to ensure the effective management of the Information Security Program unless specifically disallowed.

7. SUMMARY. This NNSA Policy consists of four sections that provide requirements for CMPC, Operations Security (OPSEC), security of SAPs, and Technical Surveillance Countermeasures (TSCM). Section A, CMPC, has three chapters. Chapter I provides the CMPC planning. Chapter II provides the CMPC requirements. Chapter III provides storage requirements for classified matter. Section B provides requirements for OPSEC. Section C presents requirements for SAPs. Section D provides requirements for the TSCM program which is a controlled Official Use Only, stand-alone document that may be obtained through the Office of DNS.

8. DEVIATIONS. Deviations from national regulations, including CFR and national-level policies, are subject to the deviation process of the governing document rather than the

Departmental deviation process. This NNSA Policy conveys no authority to deviate from law or other national-level requirements.

- a. Requests for deviations from requirements specific to the Department (Sections B to D) of this NNSA Policy must be processed in accordance with the provisions of DOE M 470.4-1 Chg. 1, *Safeguards and Security Program Planning and Management*, dated 8-26-05.
 - b. For requirements listed in Section A of this NAP, protection of some national security interests cannot be accomplished by use of measures as defined in the NNSA Policy. In such unique circumstances, the appropriate cognizant security authority may approve protection requirements tailored to that particular interest using graded protection measured described in a specific security plan.
9. DEFINITIONS. Definitions for most terms included in the NNSA DNS S&S Program may be found in DOE M 470.4-7, *Safeguards and Security Program References*, dated 8-26-05, but may also be included in this NNSA Policy if required for context. Other pertinent definitions are as follows:
- a. Cognizant Security Authority. Federal and contractor employees who have been granted the authority to commit security resources or direct the allocation of security personnel or approve security implementation plans and procedures in the accomplishment of specific work activities.
 - (1) NNSA Cognizant Security Authority (NNSA CSA). The Federal CSA responsible for inherently government functions and risk acceptance for security requirements that cannot be further delegated to the contractor.
 - (2) Cognizant Security Authority (CSA). The CSA at the contractor level. This is the level of authority granted to the contractor.
 - b. Closed Areas (CA). An area that meets the requirements of this NNSA Policy for safeguarding classified matter and/or a security interest that, because of its size, nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers. CAs are further defined in the NNSA Physical Protection NAP.
 - c. Day-lock. A practice that permits users to temporarily leave classified matter in areas where access is controlled and limited to individuals with appropriate clearance and need-to-know as documented and prescribed by the CSA.
 - d. Engineered Openings. Openings greater than 96 inches square that have been designed and constructed to allow access to storage locations for lawful purpose. Examples include, but are not limited to, door openings, window openings, and ventilation openings.
 - e. Supplemental Protection. Supplemental protection measures include additional security measures such as GSA approved security containers, intrusion detection

systems, protective force (PF) patrols, special checks or access control systems. Supplemental protection measures should be documented in the Site Security Plan (SSP) and approved by the CSA. Supplemental protection measures for nuclear material can be found in the NNSA *Physical Protection* NAP. NOTE: GSA-approved security containers and approved vaults secured with a locking mechanism meeting Federal Specification FF-L-2740 do not require supplemental protection when the CSA has determined that the GSA-approved security container or approved vault is located in an area of the facility with security-in-depth.

NOTE: When PF are authorized, the schedule of patrol is 2 hours for Top Secret matter and 4 hours for Secret matter.

10. REQUIREMENTS. Detailed requirements are included in each section of this NNSA Policy.
11. REFERENCES. References commonly used in the NNSA DNS S&S Program and the DOE S&S Program are located in DOE M 470.4-7, *Safeguards and Security Program References*, dated 8-26-05.
 - a. The following references from which the information security requirements are derived are:
 - (1) 18 U.S.C. 798, *Disclosure of Classified Information*.
 - (2) 42 U.S.C., Chapter 23, *Atomic Energy Act of 1954 (AEA)*, as amended.
 - (3) 50 U.S.C. 2426, *Congressional Oversight of Special Access Programs*.
 - (4) *National Security Act of 1947*, as amended.
 - (5) 10 CFR, *Energy*, Parts 725, 824, 1016, 1017, 1044, 1045, and 1046.
 - (6) 32 CFR, Chapter XIX, *Central Intelligence Agency*.
 - (7) 32 CFR, Chapter XX, *Information Security Oversight Office*, National Archives and Records Administration.
 - (8) 48 CFR 952.204, *Department of Energy Acquisition Regulation*, Clauses Related to Administrative Matters.
 - (9) Executive Order 12333, *United States Intelligence Activities*.
 - (a) Amended by Executive Order 13284, *Amendment of Executive Orders, and Other Actions, in Connection With the Establishment of the Department of Homeland Security*.
 - (b) Amended by Executive Order 13355, *Strengthened Management of the Intelligence Community*.

- (c) Amended by Executive Order 13470, *Further Amendments to Executive Order 12333, United States Intelligence Activities.*
- (10) Executive Order 12829, *National Industrial Security Program*, amended by Executive Order 12885, *Amendment to Executive Order 12829.*
- (11) Executive Order 12968, *Access to Classified Information*, amended by Executive Order 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*
- (12) Executive Order 13462, *President's Intelligence Advisory Board and Intelligence Oversight Board*, amended by Executive Order 13516, *Amending Executive Order 13462.*
- (13) Executive Order 13526, *Classified National Security Information.*
- (14) National Security Decision Directive 19, *Protection of Classified National Security Council and Intelligence Information.*
- (15) National Security Decision Directive 84, *Safeguarding National Security Information.*
- (16) National Security Decision Directive 298, *National Operations Security Program.*
- (17) National Disclosure Policy-1, *National Policies and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organization.*
- (18) Security Policy Board Issuance 4-97, *National Policy on Reciprocity of Use and Inspection of Facilities.*
- (19) Security Policy Board Issuance 5-97, *Guidelines for the Implementation and Oversight of the Policy on Reciprocity of Use and Inspection of Facilities.*
- (20) Secretary of Energy Delegation Order No. 00-003.00B, *To the Under Secretary for Nuclear Security*, dated 1-22-10.
- (21) NAP-1, *Establishment of a Policy Letter System for Managing Policy, Directives, and Business Practices within the National Nuclear Security Administration*, May 21, 2002.
- (22) Department of Defense Directive 5220.22, *National Industrial Security Program Operating Manual.*

(23) Department of Defense Directive 5220.22-M-Sup 1, *National Industrial Security Program Operating Manual Operating Manual Supplement*.

12. IMPLEMENTATION. Requirements that cannot be implemented within six months of the effective date of this NNSA Policy or with existing resources must be documented by the CSA and submitted to the Under Secretary for Nuclear Security/Administrator, NNSA through the NNSA CSA. A courtesy copy will be sent to the DOE Office of Health, Safety and Security. The documentation must include timelines and resources needed to fully implement this NNSA Policy. The documentation must also include a description of the vulnerabilities and impacts created by the delayed implementation of the requirements.
13. CONTACT. Questions concerning this NNSA Policy should be addressed to the Director, Office of Field Support (NA-72), National Nuclear Security Administration, Office of Defense Nuclear Security, 1000 Independence Avenue SW, Washington, DC 20585.

BY ORDER OF THE ADMINISTRATOR:

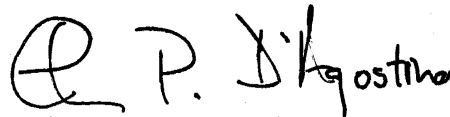

Thomas P. D'Agostino
Administrator

TABLE OF CONTENTS

INFORMATION SECURITY ii

- 1. Purpose..... ii
- 2. Background..... ii
- 3. Cancellations..... iii
- 4. Applicability iii
- 5. Authorities..... v
- 6. Responsibilities..... v
- 7. Summary..... vi
- 8. Deviations vi
- 9. Definitions..... vii
- 10. Requirements viii
- 11. References..... viii
- 12. Implementation x
- 13. Contact x

SECTION A. CLASSIFIED MATTER PROTECTION AND CONTROL..... A-1

- 1. Objectives A-1
- 2. Requirements A-2

CHAPTER I. PROTECTION AND CONTROL PLANNING.....I-1

- 1. Classified Matter Protection and Control Program Implementation I-1
- 2. Protection Strategies & Planning..... I-1
- 3. Release of Classified Information to Foreign Governments..... I-1
- 4. Training..... I-3

**CHAPTER II. CLASSIFIED MATTER PROTECTION AND CONTROL
REQUIREMENTS..... II-1**

- 1. General II-1
- 2. Classified Matter in Use..... II-3
- 3. Marking..... II-3
- 4. Marking Material II-8
- 5. Control Systems and Accountability II-8
- 6. Reproduction..... II-10
- 7. Receiving and Transmitting Classified Matter II-10
- 8. Destruction II-18
- 9. Foreign Government Information..... II-19

CHAPTER III. STORAGE REQUIREMENTS FOR CLASSIFIED MATTER	III-1
1. Storage Requirements	III-1
2. Storage—Repositories	III-2
3. Non-Conforming Storage.....	III-4
4. Permanent Burial	III-5
SECTION B. OPERATIONS SECURITY	B-1
1. Objectives	B-1
2. Requirements	B-1
SECTION C. SPECIAL ACCESS PROGRAMS.....	C-1
1. Objectives	C-1
2. Requirements	C-1
SECTION D. TECHNICAL SURVEILLANCE COUNTERMEASURES.....	D-1

SECTION A. CLASSIFIED MATTER PROTECTION AND CONTROL

1. **OBJECTIVES.** To protect and control classified matter that is generated, received, transmitted, used, stored, reproduced, permanently buried, or to be destroyed.
 - a. The following fundamental principles and objectives are the basis for this NNSA Policy:
 - (1) **Identify and Mark Asset.** The Site must ensure that all classified matter is identified with the assigned classification level, category, and applicable caveats.
 - (2) **Protect Against Identified Threats.** The Site must implement protection mechanisms necessary to address credible threats. The credible threats identified for classified matter are an insider or outsider working alone.
 - (3) **Control.** The Site must establish controls to classified matter that limit access to individuals with appropriate clearance and need-to-know.
 - (a) Need-to-know is a determination made by an authorized holder of classified information that a prospective recipient has a requirement for access to (including incidental access as defined below) knowledge or possession of the classified information to perform tasks or services essential to the fulfillment of a classified contract or program.
 - (b) Need-to-know for the National Nuclear Security Administration (NNSA) includes physical access to storage areas as well as to information.
 - (c) Incidental access may be granted to individuals who handle or come into contact with classified matter but whose job functions do not include review or other use of the classified matter.
 - (4) **Storage.** Classified matter must be stored in a General Services Administration (GSA)-approved security container or in a location that is constructed and/or configured to limit or prohibit unauthorized physical access through engineered openings. Material Access Areas (MAA) constitute adequate protection for open storage of classified matter.
 - (5) **Destruction.** Classified matter must be destroyed beyond recognition to preclude subsequent access to classified information. Destruction must be accomplished by means that provide reasonable assurance that classified information cannot be recovered.
 - (6) **Detection.** The Site must establish and maintain an Information Protection program that, together with other security disciplines, provides reasonable

assurance of detecting, assessing, and responding to unauthorized activities and anomalous conditions or events.

- b. To establish the requirements for an audit trail for all accountable classified matter.
- c. To establish required controls based on classification level (Top Secret, Secret, or Confidential) and category (Restricted Data [RD], Formerly Restricted Data [FRD]), or National Security Information) or special handling instructions or caveats.

NOTE: Implementations or controls that have not been addressed in this NNSA Policy are not automatically disallowed.

2. REQUIREMENTS.

- a. Classified matter that is generated, received, transmitted, used, stored, reproduced, permanently placed (buried according to the requirements of this NNSA Policy), or destroyed must be protected and controlled commensurate with classification level, category (if RD or FRD), and caveats (if applicable). All pertinent attributes must be used to determine the degree of protection and control required to prevent unauthorized access to classified matter.
- b. Access to classified matter must be limited to persons who possess appropriate access authorization, any formal access approvals, and who have a need-to-know as defined in this NAP for the performance of official duties.
- c. Classified matter must be stored in an authorized Property Protection Area in a GSA-approved security container, closed area, Limited Area, Exclusion Area, Protected Area, or MAA.
- d. Classified information must only be processed on information systems that have received authority to operate according to NNSA Office of the Chief Information Officer directives that establish requirements for national security systems.
- e. Audit trails must be implemented for all accountable classified matter.
- f. Buildings and rooms containing classified matter must be configured with security measures that prevent unauthorized persons from gaining access to classified matter; specifically, security measures that prevent unauthorized physical, visual, and aural access. Classified matter must be stored in a location that is configured to prohibit physical access through engineered openings by unauthorized individuals.
- g. Retention requirements for all records associated with the protection and control of classified matter must be maintained in accordance with the most current National Archives Records Administration General Records Schedule 18, *Security and Protective Services Record*.

- h. Any loss, compromise or suspected compromise of classified information, foreign or domestic, must be reported to the appropriate NNSA CSA. Classified matter that cannot be located within a reasonable period of time must be presumed to be lost until an investigation determines otherwise.

CHAPTER I. PROTECTION AND CONTROL PLANNING

1. CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) PROGRAM. To ensure the protection and control of classified information and matter, a CMPC program must be implemented to cover each National Nuclear Security Administration (NNSA) element, site, and/or facility and must be tailored to achieve the protection levels that adequately address specific site characteristics and requirements, current technology, ongoing programs, and operational needs.
2. PROTECTION STRATEGIES AND PLANNING. The Site protection measures for CMPC must be documented.
3. RELEASE OF CLASSIFIED INFORMATION TO FOREIGN GOVERNMENTS.
 - a. The National Disclosure Policy Committee (NDPC). The multi-agency NDPC, of which the Department of Energy (DOE) is a “Special Member,” governs the export of classified U.S. military information and matter to foreign governments as provided for in international agreements. To ensure uniform application of safeguards, these agreements include arrangements for the appropriate safeguarding of information and matter provided to DOE. Access to classified information and matter must be granted in accordance with established international agreements.

DOE has agreed to inform the NDPC of international agreements involving the sharing of all classified information including those made under the auspices of the Atomic Energy Act of 1954. This notification must include the provisions of security agreements that apply to the shared information. DOE is also required to coordinate with the Joint Atomic Information Exchange Group before disclosing atomic information (which includes Restricted Data [RD] and Formerly Restricted Data [FRD]).
 - b. NNSA Element. The program office is responsible for ensuring NNSA’s compliance with national-level disclosure requirements.
 - c. Criteria for Release of Classified Information. Before releasing classified information to any foreign government, DOE must determine that furnishing the classified information will result in a net advantage to the national security of the U.S. In making such a determination, the following conditions must be met:
 - (1) Determination of net advantage to the U.S. The Deputy Administrator, Defense Nuclear Nonproliferation, in coordination with the General Counsel, the DOE Office of Health, Safety and Security, the cognizant NNSA element, and other Program Offices as necessary, must determine that furnishing classified information will result in a net advantage to the national security of the U.S.

- (2) The Deputy Administrator, Defense Nuclear Nonproliferation must consult with the U.S. Department of State and other agencies and departments, as appropriate, in making this determination.
- (3) The disclosure must be consistent with the foreign policy of the U.S. toward the receiving government.
- (4) The disclosure must be limited to information necessary to the purpose for which disclosure is made.
- (5) The receiving government must have agreed, either generally or in the particular case, to the following stipulations:
 - (a) The receiving government must not release the information to a third party without the approval of the releasing party.
 - (b) The receiving government will afford the information substantially the same degree of protection afforded the information by the releasing party.
 - (c) The receiving government will use the information *only* for the purpose for which it was given.
 - (d) If the releasing party indicates any private rights (such as patents, copyrights, or trade secrets) are involved in the information, the receiving party will acknowledge such rights.
- (6) In some instances, new documents may be created that contain both U.S. classified information and foreign government information (FGI). In this case, unless there is a current agreement for cooperation (for RD or FRD) or appropriate international agreement (for National Security Information) allowing sharing of the specific categories and levels of U.S. classified information, the enhanced FGI cannot be returned to the originating government or international organization of governments.

d. Release Determination.

- (1) Initiation and Coordination. The NNSA element responsible for the classified information to be released to a foreign government must prepare the initial request and justification. The NNSA element must coordinate with the DOE Office of Health, Safety and Security; the Office of General Counsel; and the Office of Congressional and International Affairs for approval to release the classified information.
- (2) Release to Non-U.S. Citizens. The release or disclosure of FGI to non-U.S. citizens must have the prior consent of the originating government, and the individual must possess appropriate security clearance and meet need-to-know requirements.

- (3) Third-Country Transfers. The release or disclosure of FGI to any third-country entity must be coordinated through the cognizant NNSA element and DOE Office of Health, Safety and Security and have the prior consent of the originating government if required by a treaty, agreement, bilateral exchange, or other obligation.
 - (4) FGI Containing Unclassified U.S. Information. Documents containing U.S. unclassified information and FGI must be protected at the most restrictive level contained within the document.
 - (5) Returning FGI Documents. If it is necessary to return the enhanced FGI (e.g., additional U.S. information added) to the originating government or international organization, it must be handled in accordance with paragraph 3 of this Chapter.
- e. Transmittal of Classified Matter. All transmittals that involve classified information or classified matter must be made by the NNSA CSA unless the contractor has prior written authorization. If the transfer involves classified information or classified matter produced by or received from another Government agency, the cognizant NNSA element must obtain approval from the agency before transmission.
 - f. Preparation and Method of Transmission. Normally, documents intended for foreign governments must be forwarded to the receiving country's embassy in the U.S. The method of transmission of classified mail to foreign countries must be approved by the DOE Office Health, Safety and Security.
 - g. Transmittal Documentation. Copies of receipts for physical transfers must be contained in memoranda prepared by the cognizant NNSA element and maintained by the cognizant program office.
 - h. Oral Disclosure Records. Records of made and/or contemplated oral disclosures must be contained in memoranda prepared by the cognizant NNSA element and maintained by the cognizant program office.
4. TRAINING. All CMPC-related training/briefings regarding the local implementation of this NNSA Policy must be formally documented.
 - a. All personnel with security clearances whose classified matter responsibilities include access (potential or actual), originating, handling, using, storing, accounting for, reproducing, transmitting (including hand-carrying), destroying, and/or emergency reporting must receive CMPC training and/or briefings commensurate with these responsibilities prior to receiving access to classified matter and must receive refresher training and/or briefings to ensure continued reinforcement of requirements. This training and/or briefings must be tailored to the assigned duties and responsibilities of the persons receiving the training and/or briefings.

- b. Personnel with security clearances whose job responsibilities do not meet the conditions specified above (e.g., personnel employed in maintenance, janitorial, food service, and other such activities) must receive training and/or briefings and be able to identify unprotected classified matter (e.g., by classified cover sheets and classification markings) and know the associated reporting requirements.

CHAPTER II. CLASSIFIED MATTER PROTECTION AND CONTROL REQUIREMENTS

1. GENERAL. Protection and control requirements include the following:
 - a. Before classification review, matter that may be classified must be protected at the highest potential classification level and category. The originator is responsible for obtaining a classification review by a derivative or original classifier if there are any questions regarding the classification of any draft document or working paper.
 - b. When information is prepared on classified information systems, the hard-copy output (which includes paper, film, and other media) must be marked either:
 - (1) with the appropriate markings for the classification of the information as determined by a derivative classifier according to a classification review of the actual output,
 - (2) as a working paper to the accreditation level and category of the information system (see paragraph 3.p below for additional requirements that apply regarding draft and working papers), or
 - (3) according to the marking requirements for the appropriate classification of information that has been generated by a program verified and formally approved by the Designated Approving Authority (DAA) to produce consistent results. The following factors must be satisfied when exercising this option:
 - (a) The (hardcopy) output that will be produced must be fully defined and documented. The DAA must formally approve this documentation and must ensure that any subsequent output marked according to this option completely matches the planned and actual output for which the Classification Officer determined the classification level and category (if Restricted Data [RD] or Formerly Restricted Data [FRD]),
 - (b) The Classification Officer must review the fully defined output and must determine the correct classification level and category (if RD or FRD) for the information contained in the output, and
 - (c) All output must be marked with the correct classification level and category (if RD or FRD) as determined by the Classification Officer.
 - c. When matter must be sent outside the office of origin for a classification review and determination, it must be marked "DRAFT-Not Reviewed for Classification." To preclude marking every page of a document being transmitted for

classification review, it should have a “Document Undergoing Classification Review” cover sheet that is marked with the highest level and most restrictive category of information the originator believes is contained in the document.

- d. Access to classified matter in an emergency involving an imminent threat (explosion, fire, etc.) to life or defense of the homeland may be provided to individuals who are not otherwise routinely eligible for access to classified matter. If an emergency is life-threatening, the health and safety of individuals takes precedence over the need to protect classified matter from disclosure. Examples of such releases include providing law enforcement personnel with classified information concerning an improvised nuclear device found in a public place, sharing a classified U.S. Department of Energy (DOE) evaluation of the viability of a nuclear threat message with local emergency response personnel, or providing an attending physician with classified details about nuclear materials at a site to assist in the emergency treatment of a patient.
- (1) Protecting Classified Matter in Emergency Situations. Cognizant Security Authority (CSA)-approved procedures must be developed. These procedures must describe the actions (i.e., notifications, alternative storage, and protection methods) to be taken at the time of the emergency.
- (a) Every attempt must be made to minimize access by uncleared emergency response personnel to only those areas directly affected by the emergency situation.
 - (b) All unsecured classified matter must be accounted for following the emergency.
 - (c) Secure storage repositories must be inspected on return to the facility to ensure they have not been compromised.
 - (d) In all cases, contractors will notify the NNSACSA who will notify the Chief, Defense Nuclear Security (DNS) or the appropriate NNSA line management. For RD or FRD, the Chief, DNS will notify the DOE Chief, Health, Safety and Security Office.
 - (e) A description of what specific information is classified and protection requirements for the information must be provided to the recipient.
 - (f) A briefing must be provided to the recipient covering requirements for not disclosing the information and a nondisclosure agreement must be signed by the recipient.

- (2) Emergency Evacuation Drills/Tests. Emergency evacuation drill/test procedures must include protection requirements and CSA-approved procedures for protecting all classified matter from unauthorized access.
2. CLASSIFIED MATTER-IN-USE. Classified matter-in-use must be under the control of a person possessing the proper security clearance and need-to-know. Sites may authorize the use of the day-lock practice during work hours for Secret matter and below in accordance with local procedures approved by the CSA. Day-lock is a term used for classified matter-in-use during working hours and should not be confused with storage of classified matter. The authorization basis for local procedures will take into consideration, but are not limited to, the location for the use of day-lock procedures, time duration, environment in which day-lock occurs, the nature and volume of the information, and layered security.
3. MARKING. Classified matter must be marked with core markings to ensure information is appropriately protected to prevent inadvertent disclosure. Core markings include the classification level and category (if RD or FRD) and caveats, if applicable. Classified matter must be reviewed and brought up to current standards whenever it is released outside the Site or outside of an ad-hoc working group (AHWG). Marking requirements for foreign government information (FGI) are found in 9b below. Marking examples can be found in the *DOE CMPC Marking Resource*.

Classified matter in electronic form within a site's approved classified network or within an AHWG does not need to be marked as a final document. When electronic files are printed or transmitted outside the Site's classified network or AHWG, the printed or electronically transmitted matter must be marked according to current standards.

When electronic files are printed or transmitted outside the Site's classified network or AHWG, the printed matter must be marked according to current standards.

a. General.

- (1) Requirements. Classified matter, regardless of date or agency of origin, must be marked to indicate at least the classification level and category (if RD or FRD) and applicable caveats.
- (2) Document Markings. All classification markings must be distinguishable from the document text. The overall classification level (i.e., Top Secret, Secret, or Confidential) of a document must be marked on the top and bottom of the cover page (if any), the title page (if any), the first page of text, and the outside of the back cover or last page of text. DOE M 475.1-1B, *Manual for Identifying Classified Information*, dated 8-28-07, contains additional marking requirements beyond the requirements contained in this NNSA Policy. All interior pages of documents must be marked top and bottom with either:

- (a) The overall classification level and category (if RD or FRD) for the entire document, or
 - (b) The highest classification level and category (if RD or FRD) of all information on that page; or with appropriate unclassified marking (e.g., Unclassified [U], Official Use Only [OUO], Unclassified Controlled Nuclear Information [UCNI]) if there is no classified information on that page.
- (3) Unique Identification Numbers. Classified matter required to be in accountability, as defined in this Chapter, must have a unique identification number.
- b. Originating Organization and Date. The name and address of the organization responsible for preparing the document and the date of preparation must appear on the first page of all classified documents.
- c. Classification Categories. The three classification categories are RD, FRD, and National Security Information (NSI). Classified matter containing only NSI is *not* marked with a NSI admonishment.
 - (1) If the document contains RD or FRD information, the appropriate admonishment information must be marked on the first page of the document, whether cover page, title page, or first page of text and appear in the lower left corner.
 - (2) RD or FRD documents generated before July 9, 1998 are not required to be re-marked to indicate the category on each page containing RD or FRD information unless they are sent outside the Site or outside of an ad-hoc working group.
- d. Mixed Levels and Categories. When classified matter contains a mix of information at various levels and categories that causes the document to be marked at an overall level and category higher than the protection level required for any of the individual portions, a marking matrix may be used in addition to other required markings. This would allow an individual with a lower access level, such as an “L” cleared employee, to be given access to a document they might not otherwise be authorized to access if the document was only marked at the highest overall classification level and category. (For example, a document that contains Confidential RD and Secret NSI would be required to be marked as Secret RD, the highest level and most restrictive category. None of the information in the document is Secret RD). However, this may not be interpreted to authorize any individual to gain access to information that exceeds their security clearance, formal access approvals, and need-to-know.

If the marking matrix is used, the following marking, in addition to other required markings, must be placed on the first page of text. The marking should appear on

the lower right corner near the classifier information marking. If the derivative classifier places this marking on the document at the time of the classification decision, there is no need to indicate the name and title of the derivative classifier on the mixed level and category marking.

This document contains:

Restricted Data at the (e.g., *Confidential*) level.
Formerly Restricted Data at the (e.g., *Secret*) level.
National Security Information at the (e.g., *Secret*) level.

Classified by: *Name and Title*

- e. Components. When components of a document are to be issued or used separately, each major component must be reviewed and marked as a separate document. Components include annexes or appendixes, attachments, and major sections of a report. If an entire major component is unclassified, "Unclassified" must be marked at the top and bottom of the first page and a statement included (e.g., "All portions of this [annex, appendix, etc.] are Unclassified"). When this method of marking is used, no further markings are required on the unclassified component. Documents transmitted with a letter of transmittal are discussed in paragraph 3o below, Transmittal Documents.
- f. Unclassified Matter.
 - (1) Unclassified matter need not be marked unless it is essential to convey one of the following conditions:
 - (a) The matter has been reviewed for classification and does not contain classified information; or
 - (b) The matter has been properly declassified.
 - (2) If unclassified matter is marked, the Unclassified marking must be placed on the top and bottom of the front cover (if any), title page (if any), and first page of text.
- g. Portion Marking.
 - (1) NSI documents dated after April 1, 1997 must be portion-marked.
 - (2) Documents containing RD or FRD should not be portion-marked; however, if portion-marked, markings must be consistent with those defined in this Chapter.
 - (3) Portion markings must include any applicable caveats. Each section, part, paragraph, graphic, figure, subject/title, or similar portion of any such document must be accurately marked to show:

- (a) the classification level, category (if RD or FRD), and caveat (e.g., Secret/RD, Secret/FRD, Confidential/RD, Confidential/FRD, Secret, Top Secret, Secret/NOFORN), or
 - (b) that it is unclassified (e.g., UCNI, OOU, or U).
- (4) Page changes to NSI documents dated after April 1, 1997 must be portion-marked. Additionally, any NSI document that becomes active (i.e., whenever it is released outside the Site or outside of an AHWG must be portion-marked with the appropriate classification level, caveat, or unclassified.
- (5) Portions of U.S. documents containing FGI must be marked to reflect the foreign country of origin and appropriate classification level (e.g., U.K.-C, indicating United Kingdom-Confidential). FGI must be indicated in lieu of the country of origin if the foreign government indicates it does not want to be identified.
- (6) DOE M 475.1-1B, *Manual for Identifying Classified Information*, dated 8-28-07, contains portion marking and other requirements for classified matter determined to be classified by association or compilation.
- h. Subjects and Titles. Titles must be marked with the appropriate classification (level; category if RD or FRD; and other applicable caveats) or control symbol or “U” if unclassified and placed immediately after the item.
- i. Classifier Markings. Classifier marking requirements can be found in DOE M 475.1-1B.
- j. Caveats and Special Control Markings. Caveats and special control markings are placed on documents to identify special handling or dissemination requirements or to assist in describing the type of information involved or who distributed or originated the information. Caveats and special control markings and any related admonishment statements or notices should be placed above the category admonishment statement, if any, on the lower left corner of the first page (cover page, if any; title page, if any; or first page of text) and in portion markings, when required.
- k. Re-marking Upgraded, Downgraded, and Declassified Matter. Requirements for marking upgraded, downgraded, or declassified matter are contained in DOE M 475.1-1B.
- l. Re-marking Automatically Declassified Matter. Matter marked for automatic declassification must not be re-marked unless it has been reviewed and determined by an Authorized Derivative Declassifier not to contain classified information (see DOE M 475.1-1B).

- m. Classified Matter Not Automatically Declassified. For requirements see DOE M 475.1-1B.
- n. File Folders and Other Containers. File folders and other items containing classified matter, when removed from secure storage repositories, must be conspicuously marked to indicate the highest classification level of their contents.
- o. Transmittal Documents. The first page of a transmittal document must be marked with the highest level and most restrictive category (if RD or FRD) of classified information being transmitted and with an appropriate notation to indicate its classification when the enclosures are removed.
- p. Working Papers and Drafts. Classified working papers and drafts are considered to be interim production stages toward the generation of a final document. They must be:
 - (1) Dated when created,
 - (2) Marked with their overall classification level and category (if RD or FRD),
 - (3) Marked with the annotation “WORKING PAPERS” or “DRAFT”, and
 - (4) Destroyed when no longer needed.
 - (5) Working papers or drafts must be marked in the same manner prescribed for a finished document at the same classification level when:
 - (a) transmitted outside the facility, or
 - (b) retained for more than 30 days from creation for Top Secret, or 180 days from creation for Secret and Confidential.
 - (6) Filed permanently.
- q. Redacted Documents. Methods used to strike out classified information before release to persons not authorized access to the deleted information must completely obliterate the classified text, figures, etc., to prevent any form of recovery that might compromise the information. DOE M 475.1-1B contains additional redaction requirements.
- r. Other Government Agency (OGA) Not Conforming to DOE Requirements. As a rule, documents received from OGAs and foreign governments that have not been marked to conform to DOE requirements do not need to be re-marked. However, all documents received must clearly indicate a classification level and category (if RD or FRD). The sender must be contacted to resolve any marking questions.

- s. Cover Sheets. Cover sheets must be applied to all classified documents when they are removed from a secure storage repository. (Reference: Standard Forms [SF] 703–Top Secret cover sheet, 704–Secret cover sheet, and 705–Confidential cover sheet).

4. MARKING MATERIAL.

- a. Requirements. The classification level and category (if RD or FRD) and caveats, if applicable, must be conspicuously marked on all classified matter if possible. Otherwise, alternative marking methods must be used to identify the overall classification level and category (if RD or FRD). When marking is not practical, written notification of the markings must be furnished to recipients. The originator is responsible for ensuring that classified matter is marked in accordance with this NNSA Policy.
- b. Caution. Before initiating any new marking policies, it is necessary to coordinate with the production engineers. War reserve and configuration control requirements mandate strict control over what is done to specific materials—markings cannot violate these rules. Any alternative markings under consideration must be compatible with the matter being marked.
- c. Exempted Markings. Because the classifier’s annotation and origination date are maintained on the drawing specifications, these markings are not required on each piece of classified matter. Other markings such as originator identification and unique identification number (accountable matter only) do not apply because of the nature of the matter.

5. CONTROL SYSTEMS AND ACCOUNTABILITY.

- a. General. Control systems must be established and used to deter and detect unauthorized access to or removal of classified matter. Accountability systems must provide a system of procedures that provide an audit trail. Accountability, as defined below, applies regardless of the physical form of the matter (e.g., electronic, paper, or parts). Media may be removed from accountability once it has been degaussed by a National Security Agency approved degausser or other officially approved methods that comply with NNSA cyber security policy.
- b. Accountable Matter. The following are types of accountable matter:
 - (1) Top Secret matter,
 - (2) Any matter that requires accountability because of national, international, or programmatic requirements:
 - (a) national requirements such as cryptography and designated Communications Security (COMSEC);

- (b) international requirements such as North American Treaty Organization (NATO) ATOMAL, designated United Kingdom documents, or other FGI designated in international agreements;
 - (c) designated special access programs; and
 - (d) Sigma 14.
- c. Control Stations. Control stations must be established to maintain records, accountability systems, access lists (when required), and control classified matter (including facsimiles) received by and/or dispatched from facilities. Control station operators must maintain accountability systems for accountable matter.
 - (1) Accountability records are required when accountable matter is originated, reproduced, transmitted, received, destroyed, permanently buried, or changed in classification. An information management system must be established to protect and control the classified matter to ensure that classified matter is used or retained only for a lawful and authorized U.S. Government purpose. The U.S. Government reserves the right to retrieve its classified matter or to cause appropriate disposition of the matter. The information management system employed must be capable of facilitating such retrieval and disposition in a reasonable period of time.
 - (2) Records for NATO documents must be maintained separately from records of non-NATO documents. Cosmic Top Secret and all ATOMAL documents must be recorded on logs maintained separately from other NATO logs and must be assigned unique serial control numbers. Additionally, disclosure records bearing the name and signature of each person who has access are required for all Cosmic Top Secret, Cosmic Top Secret ATOMAL, and all other ATOMAL or NATO classified documents to which special access limitations have been applied.
- d. Accountable Matter. Accountability procedures must be approved by the CSA.
- e. Inventory. All accountable matter must be inventoried no less frequently than every 12 months.

Inventories must consist of a physical comparison of each item against the current inventory listing. Discrepancies must be resolved, if possible using the previously reconciled inventory and receipts, transfers, and destruction records. Each item listed in an accountability record must be verified visually.
- f. Master Files and Databases. Master files and databases created in central data processing facilities to supplement or replace Top Secret records are *not* authorized for disposal under National Archives and Records Administration's General Records Schedule 18, *Security and Protective Services Record*. These files must be scheduled on an SF 115, *Request for Records Disposition Authority*.

g. Automated Accountability Systems and Electronic Receipting.

- (1) Automated Accountability Systems. Automated accountability systems must ensure data integrity.
- (2) Electronic Receipting. Electronic receipting systems are approved as long as the following conditions are met. The system:
 - (a) is approved by the CSA;
 - (b) provides identification of both the individual and the document disposition; and
 - (c) provides adequate security controls as determined by the Site's Cyber Security Organization to ensure that no unauthorized changes are made to the system record.

6. REPRODUCTION.

- a. General. Control systems must be established to ensure that reproduction of classified matter is held to the minimum consistent with contractual and operational requirements. Classified reproduction must be accomplished by authorized personnel knowledgeable of local procedures. The use of technology that prevents, discourages, or detects the unauthorized reproduction of classified documents is encouraged.
- b. Equipment. Classified matter must be reproduced on equipment specifically approved and designated for this purpose to ensure minimal risk of unauthorized disclosure or access in accordance with CSA-approved local procedures and cyber security policy.

7. RECEIVING AND TRANSMITTING CLASSIFIED MATTER.

- a. General. If transmission of classified matter is not required by the specific terms of the contract or required for performance of the contract, contractors must obtain authorization from the NNSA CSA before transmitting classified matter outside the facility.
- b. Receiving. When classified matter is received at a facility, the following controls must apply (also see paragraph 7d below):
 - (1) Classified matter must be delivered to personnel designated to receive it at a control station with the inner envelope unopened. Procedures must be established to ensure that when classified matter is not received directly by the designated control station (regardless of the type of mail system), the inner container remains unopened.

- (2) The package must be examined for evidence of tampering and the classified contents checked against the receipt (if provided). Evidence of tampering must be maintained and reported promptly to the CSA. If the matter was received through the U.S. Postal Service, the appropriate U.S. Postal Inspector must also be notified promptly. Discrepancies in the contents of a package must be reported immediately to the sender. If the package (or container) is in order and includes a receipt, the receipt must be signed and returned to the sender.
- c. Packaging. Classified matter to be transmitted outside a facility must be double-wrapped (enclosed in opaque inner and outer containers) except as specified below. The contents of the package or shipment must be securely packaged to meet DOE and the applicable transporting agency's requirements; i.e., the U.S. Postal Service, for transmission.
- (1) Envelopes and Similar Wrappers. All classified matter physically transmitted outside facilities must be enclosed in two layers, both of which provide appropriate protection and reasonable evidence of tampering and which conceal the contents. The inner enclosure must clearly identify the classified address of the sender and the intended recipient, the highest overall classification level, and category (if RD or FRD), of the contents, and any appropriate warning notices. The outer enclosure must be the same except that no markings to indicate that the contents are classified must be visible. Intended recipients must be identified by name only as part of an attention line.
 - (2) Other Containers. The outer container must maintain the integrity of the inner container.
 - (a) As long as the item is enclosed in a double container, the matter may be wrapped or boxed in any opaque wrapping.
 - (b) If a locked briefcase is used to hand-carry classified matter of any level, the briefcase may serve as the outer container. A briefcase must not serve as the outer container for travel aboard public transportation.
 - (c) The outer container must be addressed to a classified address, return-addressed to a classified mailing address, and sealed, with no markings to indicate the contents are classified.
 - (d) If specialized shipping containers, including closed cargo transporters, are used for transmitting classified matter, the shipping container can be considered the outer container.
 - (3) Equipment Components.

- (a) If the classified matter is an internal component of a packaged item of equipment with an outside shell or body that is unclassified and that completely shields the classified internal component from view, the shell or body may be considered the inner container. If the shell or body is used as the inner container, the address and return address may be omitted.
 - (b) If the classified matter is an inaccessible internal component of a bulky item of equipment such as a missile, which cannot be reasonably packaged, no inner container is required and the outside shell or body may be considered the outer container if it is unclassified.
- d. Offsite Transmittal and Receipts. When transmitting accountable classified matter outside site/facilities (except when transmitted within an approved computer system), a receipt must be used. No receipt is necessary for non-accountable matter when hand-carried. Receipts must identify the classified contents and the names and addresses of both the sending and receiving facilities. Receipts must not contain classified information. If not practical, the receipt may be sent to the recipient with the required advance notification of shipment or may be hand-carried. When classified matter is transmitted by courier, DOE F 5635.3, *Classified Document Receipt*, or a receipt comparable in content must be used.
- (1) Receipt Information. The receipt must be prepared in triplicate and remain unclassified when completed. Two copies of the receipt must be placed in the inner container with the matter (except as noted above) and sent to the intended recipient. The third copy must be maintained by the sender until the original is signed and returned. The receipt must contain the following information:
 - (a) full names of the sender and the recipient;
 - (b) unclassified address of the sender, unless the receipt contains classified information and a classified mailing address for the sender is required;
 - (c) classified address of the recipient;
 - (d) description of the classified matter (e.g., title or other means);
 - (e) date of the matter;
 - (f) classification of the matter; and
 - (g) unique identification number, if accountable.
 - (2) Multiple Recipients. A separate receipt must be completed for each recipient regardless of the number of items for each recipient.

- (3) Facsimile Transmission. Individuals transmitting classified information through facsimile systems must confirm receipt with the intended recipient.
 - (4) Returning Receipts. The recipient of any classified matter that contains a receipt must complete the receipt and return it to the sender as soon as possible, but no longer than 30 days following receipt of matter. A copy of the receipt must be maintained with the control station records.
 - (5) Receipt Tracking. Procedures should be established for both tracking the return of receipts and the actions required if receipts are not returned.
- e. Classified Addresses.
- (1) Classified addresses must be verified through the Safeguards and Security Information Management System (SSIMS) or the Defense Security Service (DSS). If not in either system, a new classified mail channel must be established. See DOE M 470.4-1 Chg. 1, *Safeguards and Security Program Planning and Management* dated 3-7-06, for additional requirements.
 - (2) Hard-copy printouts of the SSIMS or DSS classified addresses can only be used to validate approved classified addresses for 30 calendar days from print date.
 - (3) The CSA must approve local procedures to verify classified matter channels that cannot be entered into SSIMS or DSS due to the sensitivity of the association with the receiving facility.
 - (4) NNSA Sites may use the Office of Secure Transportation (OST) Certified Program Directory (CPD) to verify approved shipment addresses for classified matter sent to "Military First Destination."
- f. Transmittal within Facilities. Classified matter may be transmitted within a facility without single or double-wrapping provided adequate security measures are taken to protect the matter against unauthorized disclosure.
- g. Transmitting Confidential Matter Outside of Facilities.
- (1) Confidential matter must be transmitted by any of the following methods or any method approved for the transmission of Secret or Top Secret matter.
 - (2) U.S. Postal Service Certified Mail is authorized within the 50 States, the District of Columbia, Puerto Rico, and U.S. territories or possessions. A return mail receipt is not required; however, if the parcel does not arrive at the appointed destination, action may be taken to obtain a receipt. A return receipt may be requested before or after delivery for all Certified

Mail and Registered Mail. NOTE: OGAs may use First Class Mail but First Class Mail is not authorized for NNSA.

- (3) The NNSA and NNSA contractors may receive Confidential matter from OGAs through U.S. Postal Service Express Mail. The use of the U.S. Postal Service Express Mail is not permitted for the transmission of Confidential matter by NNSA and NNSA contractors.

h. Transmitting Secret Matter Outside of Facilities.

- (1) Secret matter must be transmitted by one of the following ways or by any method approved for the transmission of Top Secret matter.
- (2) Postal/Mail Services.
 - (a) U.S. Postal Service Registered Mail is authorized within the 50 States, the District of Columbia, and Puerto Rico. A return receipt is not required for U.S. Postal Service Registered Mail.
 - (b) U.S. Registered Mail through Army, Navy, or Air Force Postal Service facilities, provided approval is obtained from the DOE Office of Health, Safety and Security and information does not pass out of U.S. citizen control or through a foreign postal system. This method may be used to transmit Secret matter to and from U.S. Government or U.S. Government contractor employees or members of the U.S. armed forces in a foreign country. A return mail receipt is not required.
 - (c) Canadian registered mail with registered mail receipt to and between the United States Government and Canadian Government installations in the 50 States, the District of Columbia, and Canada.
 - (d) The NNSA and NNSA contractors may receive Secret matter from OGAs through U.S. Postal Service Express Mail. U.S. Postal Service Express Mail is not permitted for the transmission of Secret matter by NNSA and NNSA contractors.
 - (e) Approved commercial express service organizations in accordance with the provisions contained in paragraph 7k below.
 - (f) Approved common carrier services with escorts who possess the appropriate security clearance in accordance with paragraph 7.1 upon approval by the CSA.

i. Transmitting Top Secret Matter Outside of Facilities. Top Secret matter must be transmitted in one of the following ways:

- (1) by the Defense Courier Service,

- (2) the U.S. Department of State Courier System if outside the United States and its territorial areas,
- (3) over approved communications networks (see DOE O 200.1A, *Information Technology*, dated 12-23-08, for requirements), or
- (4) by individuals authorized to hand-carry Top Secret matter in accordance with paragraph 7j below.

j. Hand Carrying. The following requirements apply to hand-carrying classified matter.

- (1) Local procedures must be developed describing the process for obtaining approval (including approval authority) to hand-carry outside of a site/facility and for providing notification when removing classified matter from the facility. Local hand-carry procedures must be approved by the CSA.
- (2) The removal of classified matter from approved facilities to private residences or other unapproved places (e.g., hotel or motel rooms) is prohibited.
- (3) Contingency plans for delayed arrival must cover alternative protection and storage procedures, reporting requirements, and be approved by the CSA.
- (4) Classified matter may be hand-carried outside the United States, provided the following conditions are met.
 - (a) The traveler must possess the appropriate security clearance and a diplomatic passport. Diplomatic passports can only be issued to Federal personnel attached to a mission or embassy as a tenant or performing a mission under the auspices of the U.S. Department of State.
 - (b) The traveler must obtain written authorization from the NNSA CSA.
- (5) Requirements for security screening of classified matter at airports are established by the Transportation Security Administration.

k. Approved Commercial Express Service Organizations. The use of commercial express service organizations for transmitting classified matter is restricted to emergency situations, and the matter must be delivered to and secured at the receiving location the next calendar day. At a minimum, the sender must ensure that the following conditions are met:

- (1) The use of the express service organization address for receiving deliveries from the express service has been input into SSIMS for the receiving organization.
 - (2) The address selected for the overnight/commercial express service cannot be greater than five lines, *cannot* be a post office box, and must be a street address.
 - (3) The intended recipients must be notified 24 hours in advance (or immediately if transit time is less than 24 hours) of the proposed shipments and arrival dates.
 - (4) All packages are double-wrapped before being inserted into the packaging provided by the commercial express service organization.
 - (5) In accordance with packaging requirements, commercial express service packages must not be identified as classified packages.
 - (6) The properly wrapped packages are hand-carried to the express mail dispatch center or picked up from a control station in sufficient time to allow for dispatch on the same day.
 - (7) Commercial express carrier drop boxes must not be used for classified packages.
 - (8) Facilities should include specific details regarding the use of package tracking in local procedures. The commercial express carrier may be contacted for details regarding packaging requirements.
- I. Common Carrier Services. Common carrier services include all modes and means of transport (e.g., air, rail, vehicular and intercity messenger services) excluding express service organizations. The following requirements apply to the use of such commercial services.
- (1) General.
 - (a) The contents must be securely packaged to meet NNSA and U.S. Department of Transportation requirements for transmission.
 - (b) Seals or other tamper-indicating devices approved by the CSA must be placed in a manner to show evidence of tampering on all freight and/or bulk shipments other than overnight commercial express packages. Seals must have serial numbers, which must be entered on bills of lading or other shipping papers. Seal numbers must be verified by the consignee upon arrival of a shipment.

1 Whenever practical, combination padlocks meeting Federal Specification FF-P-110, *Padlock*,

Changeable Combination, must be used to secure closed cargo areas of vehicles, vans, and railroad cars.

- 2 Shipments of Secret or Confidential matter received at common carrier terminals must be picked up by the consignee on the day of arrival unless the carrier provides continuous protective service to the address of the consignee under locally approved procedures.

(2) Assurances and Notifications.

- (a) Notification of shipments must be transmitted to the consignee before departure with 24-hour advance notice (or immediately upon dispatch if within 24 hours) to enable proper handling at the destination. At a minimum, the notification must include the nature of the shipment, means of shipment, number of seals, anticipated time and date of arrival, and requested notification if not received by a specified time.
- (b) The consignee must advise the consignor of any shipment not received within 24 hours after the estimated time of arrival furnished by the consignor or trans-shipping activities personnel. Upon receipt of such notice, the consignor must immediately begin tracing the shipment.

(3) Protective Measures. Protective measures for Departmental security shipments are as follows.

- (a) Sufficient personnel with appropriate security clearances must be tasked for a specific movement assignment to ensure continuous protection of the matter being transported.
- (b) At a minimum, the common carrier service must be required to provide the following security services:
 - 1 surveillance by an authorized carrier employee with an appropriate security clearance when the classified matter is outside the vehicle;
 - 2 a tracking system that ensures prompt tracing of the shipment while en route; and
 - 3 an alarmed or guarded storage area with immediate response by a carrier employee, commercial guard, or police officer when storage is required.

- (c) When shipments are transported by rail or motor vehicle, personnel escorting the shipments must keep the shipment car(s) under observation, maintain continuous vigilance for conditions or situations that might threaten the security of the cargo, and take appropriate actions as circumstances require. During stops or when practical and time permits, personnel escorting shipments must check the cars, container locks, and/or tamper-indicating devices.

8. DESTRUCTION.

- a. Local procedures must be established for the ongoing review of classified holdings (e.g., multiple copies, obsolete matter, classified waste) to reduce volume to the minimum necessary.
- b. If under a court order prohibiting destruction, special destruction procedures may be required. Under such circumstances, all destruction activities must be conducted in accordance with guidance provided by the NNSA Office of General Counsel and the appropriate records management organization.
- c. Classified matter must be destroyed beyond recognition to preclude subsequent access to any classified information. Electronic storage media must be destroyed in accordance with the NNSA cyber security directives. Destruction techniques vary depending on the medium on which the classified information is recorded. In general, approved destruction techniques include burning, shredding, pulping, melting, mutilating, pulverizing, or chemical decomposition. The following additional requirements must be satisfied when classified matter is destroyed.
 - (1) The CSA must approve the use of public destruction facilities and any other alternative procedures.
 - (2) If classified matter cannot be destroyed onsite, it may be destroyed at a public destruction facility. Appropriately cleared personnel must ensure classified matter is appropriately protected until destruction occurs and is properly witnessed. A record of dispatch is required when the matter is released to another cleared contractor or OGA.
- d. Equipment. Classified matter must be destroyed by equipment that has been approved by the CSA and in accordance with specific manufacturer's instructions. Residue output from all destruction processes must be inspected each time destruction is effected to ensure that established requirements have been met. The National Security Agency evaluated product lists should be reviewed when selecting destruction equipment.
 - (1) Shredders.

- (a) Crosscut shredders used for the destruction of classified paper matter and non-paper products, excluding microfilm, must produce residue with a particle size not exceeding 1 mm wide by 5 mm long. (Note exception in following paragraph.)
 - (b) Crosscut shredders purchased before December 31, 2003 that produce residue with a particle sizes not exceeding 1/32 inch wide by 1/2 inch long may continue to be used for the destruction of classified paper matter and non-paper products, excluding microfilm. However, these shredders must not be used once they cannot be repaired or restored to cut residue within the 1/32-inch wide by 1/2-inch long maximum particle dimensions.
 - (2) Pulping equipment used for the destruction of paper must be equipped with security screens with perforations of 1/4 inch or smaller.
 - (3) Pulverizing equipment (e.g. hammer mill, chopper, hybridized disintegrator) when utilized must destroy classified in a way to preclude subsequent access to classified information.
 - e. Witnesses. The destruction of accountable classified matter must be witnessed by an appropriately cleared individual other than the person destroying the matter.
 - f. Destruction Records. Destruction of accountable classified matter must be documented on DOE F 5635.9, *Record of Destruction*, or a form similar in content, which must be signed by both the individual destroying the matter and the witness.
9. FGI. The requirements in this paragraph are provided in addition to other protection and control measures in this NNSA Policy and are not applicable to NATO information. NATO information must be safeguarded in compliance with the U.S. Security Authority for NATO Instructions. Modifications to these requirements may be permitted by treaties, agreements, or other obligations with the prior written consent of the national security authority of the originating government.
- a. General. FGI must be safeguarded to provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When equivalent, standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. Confidential information, including allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information.
 - b. Classified Information Received from Foreign Governments. To ensure the protection of classified FGI in accordance with Executive Order 13526, *Classified National Security Information*, as amended, the following requirements must be met.

- (1) Handling. Classified documents received from foreign governments do not require portion-marking. Such documents generated and marked entirely by a foreign government must be protected commensurate with the classification level the foreign government specified.
- (2) Marking.
 - (a) A derivative classifier or classification officer must be contacted with any questions regarding the appropriate classification level for a FGI document.
 - (b) Documents generated by a foreign government in which U.S. information has been added must be reviewed for classification by a derivative classifier or classification officer, marked, and protected accordingly.
 - (c) If the original markings in the foreign government documents are readily recognizable as related to a U.S. classification requiring special protection and control, the documents do not require re-marking.
 - (d) If the foreign government marking is not readily recognizable as related to a U.S. classification, the foreign government document must be reviewed by a derivative classifier or classification officer, and an equivalent U.S. classification must be applied.
 - (e) If the fact that the information is FGI must be concealed, the document must be marked as if it were wholly of U.S. origin.
- (3) Confidential FGI. Unless requested by the originating government, records are not required to be maintained for Confidential FGI.
- (4) Secret FGI. Secret FGI must be entered into accountability when required by treaties or international agreements.
- (5) Top Secret FGI. Top Secret FGI must comply with the requirements in paragraph 5 above.
- (6) Confidential FGI–Modified Handling Authorized (C/FGI-MOD). If the foreign protection requirements are lower than the protection required for U.S. Confidential information, the following requirements must be met.
 - (a) Marking. If a document is determined to be C/FGI-MOD, in addition to other marking requirements above, the first page of the document must include:

1 the derivative classifier marking, unless C/FGI-MOD can be determined by foreign markings, and

- 2 the statement, “This document contains (*name of country*) (*classification level*) information to be treated as U.S. Confidential-Modified Handling Authorized.”
 - 3 the DOE F 470.9, *C/FGI-Mod Coversheet*, must be used.
- (b) Access/Need-to-Know. Access to C/FGI–MOD matter does not require DOE security clearance. However, such documents must be provided only to those who have an established need-to-know and where access is required by official duties and who are citizens from countries that have been authorized by the originating country.
- (c) Protection. C/FGI-MOD matter must be protected in the following manner:
- 1 Protection in Use. Physical control must be maintained over any matter marked as containing C/FGI-MOD matter to prevent unauthorized access to the information.
 - 2 Protection in Storage. C/FGI-MOD matter must be stored to preclude unauthorized disclosure, at least equivalent to that stipulated by the foreign government.
- (d) Reproduction. Matter marked as containing C/FGI-MOD may be reproduced without permission of the originator to the minimum extent necessary to carry out official duties.
- (e) Destruction. When C/FGI-MOD matter is to be destroyed, it must be sufficiently destroyed to preclude recovery of any of the information it contained and in a manner approved for destruction of classified matter or as approved by the NNSA CSA.
- (f) Transmission. C/FGI-MOD matter must be transmitted by means approved for transmitting classified matter unless this requirement is waived by the originating foreign government.

CHAPTER III. STORAGE REQUIREMENTS FOR CLASSIFIED MATTER

1. STORAGE REQUIREMENTS. The following physical security storage requirements apply to classified safeguards and security (S&S) interests.
 - a. Restriction on Marking Security Containers. Containers must bear no external markings indicating the level of classified matter authorized for storage.
 - b. Restrictions on Secure Storage Repositories Used for Classified Matter. Repositories used to store classified matter must not be used to store or contain other items that may be a substantial target for theft. Security containers used for storing classified matter must conform to General Services Administration (GSA) standards and specifications
 - c. Secure Storage Requirements. Classified matter must be stored in a location that is constructed and/or configured to limit or prohibit unauthorized physical access through engineered openings. Areas used for open storage of classified matter must meet the requirements below.

NOTE: The response times in this section do not apply to Special Access Programs or Sensitive Compartmented Information.

- (1) Confidential matter must be stored in the same manner prescribed for Secret or Top Secret matter, but the supplemental controls are not required.
- (2) Secret matter must be stored as described below or in any manner authorized for Top Secret matter.
 - (a) In a locked vault or in a locked GSA-approved security container.
 - (b) In a closed area equipped with intrusion detection system protection. Protective force (PF) personnel must respond within 30 minutes of alarm annunciation.
 - (c) In a Material Access Area (MAA).
 - (d) In locked, steel filing cabinets that do not meet GSA requirements (containers purchased and approved for use before July 15, 1994 may continue to be used until October 1, 2012) and are equipped with three-position, dial-type, changeable combination locks. The cabinet must be in a locked area or building within the minimum of a Limited Area (LA). In addition, one of the following supplemental controls is required:

- 1 Intrusion detection system protection that provides for response from PF personnel within 30 minutes of alarm annunciation.
 - 2 Inspection every 4 hours by PF or by cleared duty personnel when unattended.
 - (3) Top Secret matter must be stored as described below.
 - (a) In a locked, GSA-approved security container with one of the following supplemental controls:
 - 1 under intrusion detection system protection and by PF personnel responding within 15 minutes of alarm annunciation; or
 - 2 inspections by PF personnel no less frequently than every 2 hours.
 - (b) In a locked vault or closed area within a LA, Exclusion Area, Protected Area (PA), or MAA. The vault, or closed area, must be equipped with intrusion detection equipment, and PF personnel must respond within 15 minutes of alarm annunciation.
 - (c) In a locked vault or closed area, within a Property Protection Area or outside of a security area, and it must be under intrusion detection system protection. PF personnel must respond within 5 minutes of alarm annunciation.
 - (4) Nuclear weapon configurations, nuclear test and trainer devices, and nuclear-explosive-like assemblies without nuclear material must be stored in a vault or closed area located, at a minimum, within an LA. PF personnel must respond within 15 minutes of alarm annunciation.
 - d. Response Personnel. PF personnel, private security firms, or local law enforcement agency personnel must respond to intrusion detection system alarms as specified and documented in the Site Security Plan (see DOE M 470.4-1 Chg. 1, *Safeguards and Security Program Planning and Management*, dated 3-07-06, for additional information regarding S&S plans).
 - e. Alternative Storage Locations. Approved Federal records centers may be used to store classified information (see DOE M 470.4-1 Chg. 1).
2. STORAGE—REPOSITORIES. When not in use, classified matter must be stored and locked in an approved secure storage repository unless otherwise noted in this NNSA Policy. The following storage requirements apply to secure storage repositories that contain classified matter or other S&S interests.

- a. Security Containers. Secure storage repositories must not bear any external classification or other markings that would indicate the level of classified matter authorized to be stored within the container. For identification purposes, each security container must bear a uniquely assigned number on the exterior.
- b. Documentation – Standard Form (SF) 700, *Security Container Information*.
 - (1) SF 700, Part 1 must be completed for each repository, vault, or closed area approved for storing classified matter and include the names of all individuals who may be contacted if the container is found open and unattended. A record must be maintained of all individuals who have or may be granted access to the secure storage repository combination.
 - (2) The local implementation plan may dictate whether or not Block 8, *Serial No. of Lock*, must be left blank.
 - (3) SF 700, Part 1 must be affixed to the inside of the door of vaults, and closed areas containing the combination lock. For security containers, it must be placed inside the locking drawer.
 - (4) SF 700, Part 2a must be used to document the combination of the secure storage repository. It must be marked front and back with the highest level and most restrictive category (if Restricted Data [RD] or Formerly Restricted Data [FRD]) of information that may be stored within the repository and inserted in the accompanying envelope (Part 2).
 - (5) SF 700, Part 2 (envelope) must be marked front and back with the highest level and most restrictive category (if RD/FRD) of information that may be stored within the secure storage repository.
- c. Combinations. The number of personnel with access to the combination to authorized storage containers must be kept to the minimum number to reasonably accommodate the need.
 - (1) Changing Combinations. Combinations must be changed by an appropriately cleared and authorized individual as soon as practical after any of the following situations occur:
 - (a) Whenever the equipment is placed into service prior to use for the protection of classified matter.
 - (b) The termination of employment of any person having knowledge of the combination, or when the clearance granted to any such person has been withdrawn, suspended, or revoked.
 - (c) The compromise or suspected compromise of a container or its combination, or discovery of a container left unlocked and unattended.

- (d) When considered necessary by the Facility Security Officer or Cognizant Security Authority (CSA).
 - (e) Combinations used to protect North Atlantic Treaty Organization material must be changed no less frequently than 12-month intervals.
- (2) Selection of Combination Settings. Combination numbers must be selected at random. Security containers with multiple locking drawers must contain a classified combination on each drawer.
- (3) SF 701, Activity Security Check List.
- (a) The SF 701 provides a systematic means of checking end-of-day activities for a particular work area, allowing for employee accountability in the event that irregularities are discovered.
 - (b) Use of SF 701 is optional except when local security and/or implementation plans require its use for detailed end-of-day security inspections.
- (4) SF 702, Security Container Check Sheet.
- (a) The SF 702 must be used to record security checks each day a container may have been accessed by documenting the times and the initials of the person(s) who have opened, closed, or checked a particular container, room, vault, or closed area holding classified information. A sole custodian of a security container is not required to record each opening and closing of the container throughout the day. In such cases, the appropriate information must be recorded on the SF 702 the first time the container is opened that day. The container may be opened and closed as necessary without further record keeping. At the end of the day, information must be recorded indicating the final closing of the container for that day. When 24-hour operations are involved, another reasonable time period may be established to conduct end of the day/shift system checks.
 - (b) The SF 702 must be in a conspicuous location and affixed or in proximity to each security container and/or the entrance to each vault or closed area.
 - (c) The SF 702 may be destroyed 3 months following the last entry on the form.
3. NON-CONFORMING STORAGE. Non-conforming storage may only be used for classified matter that cannot be protected by the established standards and requirements

due to its size, nature, operational necessity, or other factors. For these exceptions, non-conforming storage that deters and detects unauthorized access may be used for storing classified matter.

Non-conforming storage must result in protection effectiveness equivalent to that provided to similar level(s) and categories of classified matter by standard configurations. The methods, protection measures, and procedures must be documented and approved by the CSA and documented in the site SSP.

4. PERMANENT BURIAL.

- a. Burial is an option that may be approved by the NNSA CSA for permanent placement of classified matter. In addition to meeting the requirements for non-conforming storage of classified matter, permanent burial documentation must also include:
 - (1) For active burial operations, description of the entire placement process, including protection of classified matter prior to final burial;
 - (2) Configuration of classified matter to be buried;
 - (3) Assurance that undisturbed burial is designed and will be sustained indefinitely for the buried classified matter;
 - (4) Explanation of current and future use of the burial location and all pertinent location characteristics (natural or engineered) that will limit or preclude access to the classified matter; and
 - (5) Updates to this documentation as conditions change.
- b. Classified matter that is accountable is considered to meet accountability requirements when it is permanently placed into an approved burial configuration.
- c. Inventory of previously accountable classified matter may be suspended indefinitely as long as there has been no access to the matter since it was buried.

SECTION B. OPERATIONS SECURITY

1. OBJECTIVES.

- a. To help ensure that critical program information (CPI) is protected from inadvertent and unauthorized disclosure.
- b. To provide management with the information required for sound risk management decisions concerning the protection of sensitive information.
- c. To ensure that Operations Security (OPSEC) techniques and measures are used throughout the National Nuclear Security Administration (NNSA).

2. REQUIREMENTS.

- a. An OPSEC program(s) must be implemented, covering each NNSA element, Site, and facility to ensure the protection of CPI and to assist in ensuring the protection of classified matter. The OPSEC program, in addition to ensuring the compliance with the requirements of this NNSA Policy, must also include the following activities:
 - (1) Establish a point of contact with overall OPSEC responsibilities for each Site, facility, and program office whose name and contact information will be provided to the DOE Office of Health, Safety and Security.
 - (2) Ensure OPSEC point of contact participation in the development of local implementation training and/or briefings tailored to the job duties of the individual employees.
 - (3) Development and execution of a comprehensive OPSEC awareness program that includes regular briefings to ensure that personnel are aware of their responsibilities in support of the OPSEC program. These briefings provide local implementation of requirements and may be integrated into, or provided in conjunction with, required security briefings (e.g., new-hire initial briefings, comprehensive or annual refresher briefings).
 - (4) Participation in self-assessments to ensure the requirements to protect and control classified matter and CPI are being followed in all areas and that employees are aware of their responsibilities.
 - (5) Provision of information concerning deviations (e.g., variances, waivers, and exemptions) involving the OPSEC program to the DOE Office of Health, Safety and Security and to the Chief, Defense Nuclear Security (DNS) when involving NNSA facilities, in a timely fashion, to include implementation and expiration of such actions. This may be accomplished through the field or Site office manager as appropriate.
 - (6) Promulgation of new OPSEC requirements to all affected employees.

- (7) Interaction and coordination with DOE Office of Health, Safety and Security on OPSEC National and Departmental requirements interpretation and local implementation activities. Interaction and coordination between NNSA facilities and the DOE Office of Health, Safety and Security is through the Chief, DNS.
- b. OPSEC plans must be developed for programs and operations and approved by the Cognizant Security Authority (CSA).
- c. OPSEC plans must be reviewed and updated annually (at least every 12 months).
- d. CPI, formerly known as critical sensitive information, must be identified including operational and programmatic data that would have a negative impact on national security and/or Departmental operations if unauthorized disclosure should occur. The CPI must be—
 - (1) prioritized according to the level of impact posed by an unauthorized disclosure. The CPI may be supported by a list of indicators that, when aggregated and analyzed, inappropriately reveal elements of the CPI.
 - (2) reviewed on a continuing basis. Results of the CPI reviews must be documented and maintained in program files.
- e. OPSEC assessments must be conducted at facilities having Category I special nuclear material (SNM) (or credible roll-up of Category II to a Category I quantity), Top Secret or Special Access Program (SAP) information within their boundaries. OPSEC assessments must be conducted at other facilities involved in creating, handling, storing, processing, transmitting, or destroying CPI as deemed necessary by the CSA.
 - (1) Either the programmatic or facility approach may be used to conduct OPSEC assessments. If the facility approach is used, all activities at the facility must be included in the assessment. If the programmatic approach is used, all activities within the program must be included in the assessment.
 - (2) When using the programmatic approach, the assessment team must ensure that CPI pertaining to Category I SNM (or credible roll-up of Category II to a Category I quantity), Top Secret matter, or SAPs are assessed. Schedule and priority for conducting assessments will be based on CPI, threat assessments, risk management principles, recommendations received from the local OPSEC program, and direction from NNSA line management.

- f. OPSEC Reviews.
- (1) Reviews must be conducted to identify changing priorities in the local OPSEC program. OPSEC reviews are limited information-gathering activities to provide the data necessary to schedule and implement OPSEC actions. Results of OPSEC reviews must be documented.
 - (2) OPSEC reviews of sensitive activities and facilities must be conducted whenever the following criteria are met:
 - (a) New construction is planned for a facility that will process or store classified or sensitive information or matter.
 - (b) New sensitive activities are initiated or existing programs incur significant changes.
 - (c) A sensitive program or activity has not been the subject of an OPSEC assessment or OPSEC review for the preceding 2 years.
- g. Information to be posted to publicly available websites.
- (1) Before any information generated by or for the Federal Government (Government Information) is placed on a NNSA, NNSA contractor, or subcontractor website or is otherwise made available to the public, it must be reviewed to ensure that it does not contain classified information or CPI. Before NNSA employees, NNSA contractors, or subcontractors post Government Information to a personal or non-NNSA website, it must also be reviewed for the same concerns. The review process must include a multi-layer review to ensure suitability of the information for worldwide public release.
 - (2) Automated analysis tools should be used to assist in the review of information to determine if it is appropriate to release it to the public. Certain categories of unclassified information are generally recognized as unsuitable for public release. These include, but are not limited to, Official Use Only information, privacy information, protected Cooperative Research and Development Agreement information, Unclassified Controlled Nuclear Information, and Export Control Sensitive Subjects information. Due to the diversity of information that must be considered within NNSA, a robust review and approval process must be conducted using the following evaluation factors for determining suitability for release of information to the public. Evaluation factors include:
 - (a) Sensitivity. If the information is released to the public, it must not reveal or identify sensitive information, activities or programs.

- (b) Risk. Information that may be used by adversaries to the detriment of employees, the public, the Department or the nation must not be approved for release. This determination must be based on sound risk management principles focused on preventing potential adverse consequences.
- (3) Heads of NNSA elements must document a program element position that identifies categories of information deemed inappropriate for public release and establishes review and approval procedures for all information being considered for release.
- (4) Local procedures must be established for conducting information reviews and acquiring approval according to direction from the head of their respective NNSA element. These procedures must identify specific information and information categories considered unsuitable for release to the public.

SECTION C. SPECIAL ACCESS PROGRAMS

1. OBJECTIVES. To establish requirements for Special Access Programs (SAP) authorized for use within the Department. (NOTE: Terms and activities such as Limited Access, Controlled Access, and Limited Distribution programs are not authorized.)
2. REQUIREMENTS.
 - a. All SAPs must be approved by the Secretary or Deputy Secretary based upon the recommendation of the SAP Oversight Committee (SAPOC), which manages and oversees the development of SAP security policies and procedures outlined in DOE M 471.2-3B, *Special Access Program Policies, Responsibilities and Procedure*, dated 10-29-07.
 - b. SAPs must be limited to acquisition, operations, support, and intelligence activities.
 - c. U.S. Department of Energy (DOE) and non-DOE (Work for Others) SAPs, with the exception of intelligence SAPs, must be registered manually (not in the Safeguards and Security Information Management System) through the established facility clearance process using DOE F 470.2, *Facility Data Approval Record (FDAR)* and DOE F 470.1, *Contract Security Classification Specification*, Department of Defense Form 254, *Contract Security Classification*, or form similar in content. For additional information regarding the FDAR process, see DOE M 470.4-1 Chg. 1, *Safeguards and Security Program Planning and Management* dated 3-7-06. The FDAR and other forms must be classified in accordance with classification guidance. SAPs must be manually registered through the SAP Security Coordinator with the National Nuclear Security Administration (NNSA) SAP Security Program Manager. Intelligence SAPs must be manually registered with the Office of Intelligence and Counterintelligence (IN) in accordance with instructions provided by IN. Registration of all Intelligence SAPs, other than those housed in a sensitive compartmented information facility, will be coordinated between the NNSA SAP Security Program Manager and the Intelligence Work for Others Coordinator.
 - d. SAP facilities, work areas, and all activities must be surveyed according to DOE M 470.4-1 Chg. 1, by the cognizant SAP Security Coordinator in coordination with the cognizant program office and/or sponsor. Intelligence SAPs must be surveyed by IN in conjunction with the Sponsor. Independent oversight inspections must be performed for Departmental programs in accordance with DOE M 471.2-3B.
 - e. Protection program planning documents, including security plans and standard operating procedures, must comply with established SAP policies and program security manuals.

- f. Any possible or probable loss, compromise, or unauthorized disclosure of SAP information must be reported to the appropriate Government Program Manager, Government Program Security Officer, DOE SAP Security Program Manager (or Cognizant SAP Security Coordinator) and the SAPOC's Executive Secretary in accordance with established procedures. DOE M 470.4-1 Chg. 1, contains additional requirements.

SECTION D. TECHNICAL SURVEILLANCE COUNTERMEASURES

This Section is Official Use Only

Please contact the Office of Defense Nuclear Security (202) 586-8900 to
request a copy of Section D

National Nuclear Security Administration
Washington, D.C.

ADMIN CHANGE

NAP 70.4 Chg 1

Approved: 7-02-10
Admin Chg 1: 7-20-11

SUBJECT: INFORMATION SECURITY

LOCATION OF CHANGES:

Page	Paragraph	Changed	To
iii	3.a.	This NNSA Policy does not cancel any NNSA-issued policy. It does, however, replace DOE M 470.4-4A for application to the NNSA's Information Security Program.	This NNSA Policy does not cancel any NNSA-issued policy. It does, however, replace DOE M 470.4-4A, and its successors, for application to the NNSA's Information Security Program.

BY ORDER OF THE ADMINISTRATOR:



TERESA M. TYNER
Director
Office of Business Operations
Office of Management and Budget