

MANUAL

DOE M 470.4-4

Approved: 8-26-05

Chg 1: 6-29-07

INFORMATION SECURITY



U.S. DEPARTMENT OF ENERGY
Office of Health, Safety and Security

Vertical line denotes change.

AVAILABLE ONLINE AT:
www.directives.doe.gov

INITIATED BY:
Office of Health, Safety and Security

INFORMATION SECURITY

1. PURPOSE. Establish security requirements for the protection and control of information and matter required to be classified or controlled by statutes, regulations, or Department of Energy (DOE) directives. The information security program includes Classified Matter Protection and Control (CMPC); Operations Security (OPSEC); Technical Surveillance Countermeasures (TSCM); security of Foreign Government Information (FGI) and Sensitive Compartmented Information (SCI); security of special access programs; and that unclassified information required to be controlled by statutes, regulations, or DOE directives, generally referred to as unclassified controlled information.

Although separate from the safeguards and security (S&S) information security program, the Department's cyber security program operates under the same basic protection principles. The cyber security program (including both classified and unclassified cyber security) is administered by the Department's Chief Information Officer.

2. OBJECTIVES.
 - a. Effect the policy in DOE P 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*, by integrating information security into DOE operations as determined by line management, and according to sound risk management practices. (DOE Policy 470.1, *Integrated Safeguards and Security Management Policy [ISSM]*, is the Department's philosophical approach to the management of the S&S Program. A principal objective of the ISSM Program is to integrate S&S into management and work practices at all levels, based on program line management's risk management-based decisions, so that missions may be accomplished without security events, such as interruption, disruption or compromise. This approach includes individual responsibility and implementation of the security requirements found in this Manual.)
 - b. Establish requirements for protecting classified and unclassified controlled information.
 - c. Ensure that any release of classified information to the public complies with applicable release restrictions or only involves information that has been formally and officially declassified by an appropriate declassification authority, and that its release is otherwise permitted by applicable laws or regulations.
 - d. Ensure that unclassified controlled information is not released to the public without review and approval.
 - e. Establish graded protection measures for each classification level (Confidential, Secret, and Top Secret).

3. PROGRAM INTEGRATION. The information security program must be integrated with other programs such as S&S program planning and management, physical protection, protective force, personnel security, and nuclear material control and accountability. Additionally, the activities and requirements in the weapons surety, foreign visits and assignments, safety, emergency management, cyber security, intelligence, and counterintelligence programs should be considered in the implementation of this Manual.
4. CANCELLATIONS. The directives listed below are canceled. Cancellation of a directive does not by itself modify or otherwise affect any contractual obligation to comply with such a directive. Canceled directives that are incorporated by reference in a contract remain in effect until the contract is modified to delete the reference to the requirements in the canceled directives. The publication of this Manual incorporates or cancels all previous memoranda or letters that were issued by the Office of Health, Safety and Security or its predecessor organizations that established policy.
 - a. DOE O 471.2A, *Information Security*, dated 3-27-97
 - b. DOE M 471.2-1C, *Classified Matter Protection and Control*, dated 4-17-01
 - c. DOE M 471.2-4, *Technical Surveillance Countermeasures*, dated 2-6-04, except for the classified annex
 - d. DOE M 471.2-1B, *Classified Matter Protection and Control*, dated 1-06-99
5. APPLICABILITY.
 - a. Departmental Elements. Except for the exclusion in paragraph 5.c., this Manual applies to all Departmental elements. (Go to <http://www.directives.doe.gov/pdfs/reftools/org-list.pdf> for the current listing of Departmental elements. This list automatically includes all Departmental elements created after the Order is issued.)

The Administrator of the National Nuclear Security Administration (NNSA) will assure that NNSA employees and contractors comply with their respective responsibilities under this Manual.
 - b. Contractors.
 - (1) The Contractor Requirements Document (CRD), Attachment 1, sets forth requirements of this Manual that will apply to site/facility management contracts that include the CRD.
 - (2) The CRD must be included in the site/facility management contracts that involve classified information or matter, or nuclear materials and contain DOE Acquisition Regulation (DEAR) clause 952.204-2, titled *Security Requirements*.

- (a) Departmental elements must notify contracting officers of affected site/facility management contracts to incorporate this directive into those contracts.
 - (b) Once notified, contracting officers are responsible for incorporating this directive into the affected contracts via the *Laws, Regulations, and DOE Directives* clause of the contracts once notified.
- (3) A violation of the provisions of the CRD relating to the safeguarding or security of Restricted Data 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. 228b.). The procedures for the assessment of civil penalties are set forth in Title 10, Code of Federal Regulations (CFR), Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations*, (10 CFR Part 824).
- (4) As stated in DEAR clause 970.5204-2, titled *Laws, Regulations, and DOE Directives*, regardless of the performer of the work, site/facility contractors with the CRD incorporated into their contracts are responsible for compliance with the CRD. Affected site/facility management contractors are responsible for flowing down the requirements of the CRD 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 CRD and only incur costs that would be incurred by a prudent person in the conduct of competitive business.
- (5) This Manual does not automatically apply to other than site/facility management contracts. Application of any of the requirements of this Manual to other than site/facility management contracts will be communicated as follows:
 - (a) Heads of Field Elements and Headquarters Departmental Elements. Review procurement requests for new non-site/facility management contracts that involve classified information or matter, or nuclear materials and contain DEAR clause 952.204-2, *Security Requirements*. If appropriate, ensure that the requirements of the CRD of this Manual are included in the contract.
 - (b) Contracting Officers. Assist originators of procurement requests who want to incorporate the requirements of the CRD of this Manual in new non-site/facility management contracts, as appropriate.

- c. Exclusion. In accordance with the responsibilities and authorities assigned by Executive Order 12344 and to ensure consistency throughout the joint Navy and DOE organization of the Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors will implement and oversee all requirements and practices pertaining to this Manual for activities under the Deputy Secretary's cognizance.
6. DEVIATIONS. Deviations from the requirements in this Manual must be processed in accordance with DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.
7. DEFINITIONS. Terms commonly used in the program are defined in the S&S Glossary in DOE M 470.4-7, *Safeguards and Security Program References*. In addition to those in the Glossary, the following definitions are provided for use in this Manual.
 - a. DOE line management refers to DOE and NNSA Federal employees who have been granted the authority to commit resources or direct the allocation of personnel or approve implementation plans and procedures in the accomplishment of specific work activities.
 - b. Line management refers to DOE and NNSA Federal and contractor employees who have been granted the authority to commit resources or direct the allocation of personnel or approve implementation plans and procedures in the accomplishment of specific work activities.
 - c. DOE cognizant security authority refers to DOE and NNSA Federal 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.
 - d. Cognizant security authority refers to DOE and NNSA 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.
 - e. For the purposes of this Manual, the Office of Health, Safety and Security refers to the DOE Office of Health, Safety and Security.

IMPLEMENTATION. Requirements that cannot be implemented within 6 months of the effective date of this Manual or with existing resources must be documented by the cognizant security authority and submitted to the relevant program officers; the Under Secretary, the Under Secretary for Science, or the Under Secretary for Nuclear Security/Administrator, NNSA; and the Office of Health, Safety and Security. The documentation must include timelines and resources needed to fully implement this Manual. The documentation must also include a description of the vulnerabilities and impacts created by the delayed implementation of the requirements.

8. CONTACT. Questions concerning this Manual should be directed to the Office of Health, Safety and Security at 202-586-3345.

BY ORDER OF THE SECRETARY OF ENERGY:



CLAY SELL
Deputy Secretary

CONTENTS

SECTION A—CLASSIFIED MATTER PROTECTION AND CONTROL

1. Objectives.....	1
2. Requirements.....	1

CHAPTER I. PROTECTION AND CONTROL PLANNING

1. Classified Matter Protection and Control Program Implementation.....	I-1
2. Program-Specific Characteristics.....	I-1
3. Threat.....	I-2
4. Protection Strategies.....	I-2
5. Planning.....	I-2
6. Training.....	I-2
7. Graded Approach to Protection.....	I-3
8. Storage—Containers.....	I-4

CHAPTER II. CLASSIFIED MATTER PROTECTION AND CONTROL REQUIREMENTS

1. General.....	II-1
2. Classified Matter In Use.....	II-5
3. Marking.....	II-6
4. Control Systems and Accountability.....	II-43
5. Reproduction.....	II-50
6. Receiving and Transmitting Classified Matter.....	II-53
7. Contract Closeout/Facility Clearance Termination.....	II-72
8. Destruction.....	II-75
9. Foreign Government Information Program.....	II-80
10. Material.....	II-91

CHAPTER II FIGURES

Figure II-1. Cover Sheet for a Document Undergoing Classification Review.....	II-3
Figure II-2a. DOE F 1325.7, Telecommunication Message.....	II-28
Figure II-2b. DOE F 1325.7, Telecommunication Message Instructions.....	II-29
Figure II-3. Example Markings for A Classified Microfilm Reel.....	II-31
Figure II-4. Example Markings for Classified File Folders.....	II-38
Figure II-5. Notice Regarding Restrictions on Reproducing Classified Information.....	II-52
Figure II-6. Classified Reproduction Procedural Instructions.....	II-53
Figure II-7a. DOE F 5635.3, Classified Document Receipt.....	II-58
Figure II-7b. DOE F 5635.3, Classified Document Receipt, OMB Burden Disclosure Statement.....	II-59

CONTENTS (continued)

Figure II-8a. Statement of Security Assurance	II-62
Figure II-8b. Statement of Security Assurances, Instructions	II-63
Figure II-9. Example Certificate of Nonpossession of Classified Matter.....	II-74
Figure II-10. Example Certificate of Possession of Classified Matter	II-75
Figure II-11a. DOE F 5635.9, Record of Destruction	II-79
Figure II-11b. DOE F 5635.9, Record of Destruction, OMB Burden Disclosure Statement ..	II-80
Figure II-12. DOE F 5639.4, C/FGI-Mod Confidential Foreign Government Information—Modified Handling Authorized.....	II-88
<u>CHAPTER II TABLES</u>	
Table II-1. National Security Information Historical Document Review Markings	II-22
Table II-2. Foreign Equivalent Classification Markings	II-33
<u>CHAPTER III. PROTECTION OF CLASSIFIED MATTER</u>	
1. General Requirements.....	III-1
2. Storage Requirements	III-1
SECTION B—OPERATIONS SECURITY	
1. Objectives.	1
2. Requirements.	1
SECTION C—SPECIAL ACCESS PROGRAMS	
1. Objectives	1
2. Requirements.	1
SECTION D—UNCLASSIFIED CONTROLLED INFORMATION	
1. Objectives	1
2. Requirements.	1
SECTION E—TECHNICAL SURVEILLANCE COUNTERMEASURES PROGRAM	
APPENDIX 1. POSITIVE CONTROL OF REPOSITORY ACCESS WITH XO-SERIES LOCKS	
ATTACHMENTS	
1. Contractor Requirements Document.....	Attachment 1-1

SECTION A—CLASSIFIED MATTER PROTECTION AND CONTROL

1. OBJECTIVES.

- a. To protect and control classified matter that is generated, received, transmitted, used, stored, reproduced, or destroyed.
- b. To establish 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 (NSI)) or special handling instructions or caveats.

2. REQUIREMENTS.

- a. Classified information and matter that is generated, received, transmitted, used, stored, reproduced, or destroyed must be protected and controlled.
- b. Audit trails must be implemented for all accountable classified matter.
- c. Classification level, category and other information attributes must be used to determine the degree of protection and control required to prevent unauthorized access to classified information and matter.
- d. Controls must be established to prevent, deter, and detect unauthorized access to classified matter.
- e. Custodians and authorized users of classified matter are responsible for protecting such matter.
- f. Buildings and rooms containing classified matter must be provided the security measures necessary to deter unauthorized persons from gaining access to classified matter; specifically, security measures that prevent unauthorized visual and/or aural access.
- g. Classified information may be disclosed only to individuals who have appropriate access authorization for the level and category of the information involved, all required formal access approval(s), and a legitimate need-to-know.
- h. Detailed requirements for marking, accountability and control systems, reproduction, receipt, transmission, and destruction are contained in Chapter II.

CHAPTER I. PROTECTION AND CONTROL PLANNING

1. CLASSIFIED MATTER PROTECTION AND CONTROL (CMPC) PROGRAM IMPLEMENTATION. To ensure the protection and control of classified matter, a CMPC program must be implemented to cover each Program Office, site, and facility. The CMPC program, in addition to ensuring the compliance with the requirements of this Manual, must also include the following activities:
 - a. Establishment of a point of contact with overall CMPC responsibilities for each site, facility, and program office whose name and contact information shall be provided to the Office of Health, Safety and Security.
 - b. CMPC point of contact participation in the development of local implementation training and/or briefings tailored to the job duties of the individual employees.
 - c. Development and execution of a comprehensive CMPC awareness program that includes regular briefings to ensure personnel are aware of their responsibilities in support of the CMPC program. These briefings provide local implementation of National and Departmental requirements and may be integrated into or provided in conjunction with required security briefings (e.g., new hires' initial briefings, comprehensive or annual refresher briefings).
 - d. Participation in self-assessments to ensure the National, Departmental, and local requirements to protect and control classified information are being followed in all areas and employees are aware of their responsibilities.
 - e. Provision of information concerning policy deviations (e.g., variances, waivers, and exceptions) involving the CMPC program to the Office of Health, Safety and Security, and to the Associate Administrator for Defense Nuclear Security when involving National Nuclear Security Administration (NNSA) facilities, in a timely fashion, to include implementation and expiration of such actions.
 - f. Promulgation of new CMPC requirements to all affected employees in a timely fashion.
 - g. Interaction and coordination with Office of Health, Safety and Security on CMPC National and Departmental requirements interpretation and local implementation activities. Interaction and coordination between NNSA facilities and the Office of Health, Safety and Security is through the Associate Administrator for Defense Nuclear Security.
2. PROGRAM-SPECIFIC CHARACTERISTICS. Classified matter protection programs must be tailored to address specific site characteristics and requirements, current technology, ongoing programs, and operational needs. These programs must also be customized to achieve protection levels that adequately and cost-effectively reduce risk.

3. THREAT. DOE O 470.3, *Design Basis Threat (DBT) Policy*, must be used in conjunction with local threat guidance and vulnerability assessments for protection and control program planning.
4. PROTECTION STRATEGIES.
 - a. Strategies for the protection and control of classified matter must incorporate the applicable requirements established in this Section. In addressing the threat to Departmental assets, emphasis must be placed on security systems that will prevent, detect, or deter unauthorized disclosure or modification, loss of availability, and unauthorized removal of classified matter.
 - b. Safeguards and security (S&S) systems and critical system elements must be performance tested to ascertain their effectiveness in providing countermeasures to address the DBT and local threat guidance.
5. PLANNING. Circumstances unique to each facility will determine how requirements set forth in Departmental directives are accomplished. Local procedures must ensure that these requirements are fulfilled in a consistent and uniform manner.
 - a. Site Safeguards and Security Plans (SSSP). The details of site protection measures for classified matter must be addressed in the SSSP, which is required by DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.
 - b. Security Plans. At locations where a SSSP is not required due to the limited scope of S&S interests, a site security plan (SSP) must be developed to describe the site protection measures for the CMPC program.
6. TRAINING. The Office of Health, Safety and Security ensures that CMPC training standards, curricula and courses are developed by the Department of Energy (DOE) National Training Center (NTC) in accordance with National and Departmental requirements. This training must be tailored to the assigned duties and responsibilities of the persons receiving training. (Specific training requirements, in addition to those stated in this Section, are included in DOE M 470.4-1, *Safeguards and Security Program Planning and Management*.)
 - a. Each individual identified as a CMPC point of contact, according to Section A, chapter 1, paragraph 1., must receive initial training developed by the NTC, as specified above, with CMPC refresher training every 4 years through direct correspondence, or on-line training.
 - b. Other personnel may also receive the NTC-developed training, or they may receive local CMPC training and/or briefings, to include local implementation requirements developed and provided by, or at a minimum, approved by the local CMPC point of contact as part of the local CMPC program.

- c. Each DOE cognizant security authority must ensure that all training and/or briefings for local CMPC implementation at locations/activities under their cognizance is consistent with National and Departmental policy and that those individuals identified in this Section receive training as required by this Manual.
 - d. All personnel whose responsibilities include generating, handling, using, storing, reproducing, transmitting (including hand carrying), and/or destroying classified matter must receive CMPC training and/or briefings, commensurate with these responsibilities, prior to receiving access to classified matter, and refresher training and/or briefings to ensure that such matter is not lost or compromised.
 - e. Personnel with access authorizations whose job responsibilities do not meet the conditions specified in paragraph d. 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.
 - f. The following subject areas, as they relate to specific job responsibilities, must be included in initial and refresher CMPC training or briefings: generation and marking, physical protection and storage, reproduction, accountability, transmission (including hand carrying), destruction, incident reporting, and emergency procedures.
 - g. Additional detailed CMPC training and/or briefings beyond the basic initial training and/or briefings must be provided to custodians and control station operators to prepare them to perform their duties. After the initial detailed CMPC training and/or briefings, these individuals must receive detailed refresher training and/or briefings in addition to the annual refresher briefing at least once every 24 months.
7. GRADED APPROACH TO PROTECTION. By a graded approach, DOE intends that, when developing and implementing protection and control programs, the level of effort and magnitude of resources expended for the protection of a particular S&S interest should be commensurate with its importance or the effect of its loss, theft, compromise, and/or unauthorized use. Interests whose loss, theft, compromise, and/or unauthorized use would have serious impacts on National security and/or the health and safety of DOE and contractor employees, the public, the environment, and/or DOE or other Government programs must be given the highest level of protection (e.g., information that would help an adversary to develop a nuclear weapon or would assist an unauthorized person to bypass use-control systems could have consequences so grave as to demand the highest attainable standard of security). Protection measures for other S&S interests are graded accordingly. The results of asset valuations, threat analyses, and vulnerability assessments should be considered (along with the acceptable level of risk and any uncertainties) to determine the level of risk and what protection measures are to be applied. The process and results of these and other methods used to determine risk and

associated mitigation strategies must be documented (e.g., in an SSSP, SSP or in program files).

8. STORAGE—CONTAINERS. When not in use, classified matter must be stored in a security container, vault, or vault-type room (VTR), unless otherwise noted in this Manual or DOE M 470.4-2, *Physical Protection*. The following storage requirements apply to those security containers, vaults, or VTRs that contain classified matter or other S&S interests.

a. Security Containers.

(1) General.

- (a) The outside of security containers must not be marked to indicate the classification level of the contents (i.e., Top Secret, Secret, or Confidential).
- (b) Security containers, vaults, and VTRs used to protect S&S interests must be kept locked when not under direct supervision of an authorized individual.

(2) Accountable Classified Removable Electronic Media (ACREM).

- (a) All ACREM must be in a Limited Area or higher security area when stored¹. Vaults or VTRs that are used to store ACREM must be configured to provide limited access to ACREM by only the ACREM custodian(s) or alternate ACREM custodian(s).

1 In vaults and VTRs, protection must be at least equivalent to storage in file cabinets which remain locked, except when ACREM is being retrieved or returned to storage, to ensure that only the ACREM custodian(s) and alternate ACREM custodian(s) have access to ACREM in its storage location.

2 Keys and equivalent mechanisms allowing access to ACREM must be strictly controlled and the control system must be documented.

- (b) GSA-approved repositories used to store ACREM not located in a vault or VTR must remain locked except when ACREM is being retrieved or returned to storage.

¹ If operational needs absolutely require storage of CREM which is required to be marked as Secret outside a Limited Area or higher, then the CREM must be placed into accountability [see Chapter II, 4b(2)]. These circumstances must be identified and justified through documented DOE CSA-approved procedures prior to implementation.

- |
- (c) Each time a security container being used to store ACREM, that is located outside a vault or VTR is closed, a seal must be affixed, and this action documented according to locally approved procedures, to provide positive evidence of opening/tampering. Alternatively, if the security container is equipped with a Mas-Hamilton XO-series lock, the following procedures must be followed:
- 1 Prior to opening the container, the authorized opener will operate the lock so as to display the number of prior openings. The number indicated should correspond to that noted on the Standard Form (SF) 702 from the previous opening. (If the number has advanced by one or more integers, the custodian will be alerted that the container had been opened with no record of such on the SF 702.)
 - 2 The number of repository openings will be noted sequentially with other entries on the SF 702 with the date and time of the opening and the opener's initials. Each opening number, as recorded on the XO-series lock, must be logged on the SF 702, along with the other required information, to provide a complete and up-to-date record of who opened the repository and when they did so. The lock opening numbers may be written immediately below each associated repository opening record on the SF 702. The new number (previous total plus one) will be noted on the SF 702 when opening the container, along with (and on the line immediately below) the associated date, time, and opener's initials.
 - 3 Additional information and requirements are included in Appendix 1, Positive Control of Repository Access with XO-Series Locks.

b. Documentation.

(1) SF 700, Security Container Information.

- (a) SF 700, part 1, must be completed for each security container, room, vault, VTR, or other location approved for storing classified matter, including the names of all individuals who have or may be granted access to the combination for the security container, vault, or VTR.

- 1 The local implementation plan may dictate whether or not Block 8, *Serial No. of Lock*, must be left blank.

- 2 Emergency notification personnel and security container custodians must be listed on each SF 700.
 - 3 The top copy must be affixed to the inside of the door of vaults and VTRs containing the combination lock. For security containers, it must be placed on the inside (back of the front) of the locking drawer.
- (b) SF 700, part 2a, must be used to document the combination of the security container, vault, or VTR. It must be marked top and bottom with the highest level, and category (if Restricted Data [RD] or Formerly Restricted Data [FRD]), of information that may be stored within it, and inserted in the accompanying envelope (part 2).
 - (c) SF 700, part 2, (envelope), once completed and sealed must be forwarded to central records for storage that prevents access by any individual who does not possess the same access authorization, any required formal access approval, and need-to-know. If the combination protects information requiring additional access approvals (e.g., Sigma 14, Sigma 15, Special Access Program (SAP) information, or Sensitive Compartmented Information (SCI)), the part 2 must not be sent to central records unless all individuals at that location possess the same access authorization, any required formal access approval, and need-to-know. If the central records location cannot accept the part 2, an alternative storage location will be required. Envelopes that contain combinations for ACREM containers must be marked to prevent release of the enclosed combination to other than appropriate ACREM custodians, alternate custodians and emergency notification personnel.
- (2) Check Systems. A check system must be established to ensure that classified matter has been properly stored and that security containers, vaults, VTRs, or other locations approved for classified storage have been secured at the end of the day or shift. When 24-hour operations are involved, another reasonable time period for system checks may be established. The check system(s) used at a site or facility must be documented in local security and/or implementation plans.
 - (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 the SF 701 is optional except when local security and/or implementation plans require its use for detailed end-of-day security inspections.
- (c) Completed SF 701s must be maintained according to the National Archives and Records Administration (NARA) General Records Schedule (GRS) 18.

(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 VTR 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. If two or more persons share the container, including containers used to store Classified Removable Electronic Media (CREM), each opening and closing must be duly recorded.
- (b) The SF 702 must be used for any container used to store ACREM, including locked drawers or file cabinets in vaults and VTRs and those that use XO-Series locks as described in Appendix 1, Positive Control of Repository Access with XO-Series Locks.
- (c) The SF 702 must be affixed to each container and the entrance to each vault or VTR. When it is not feasible to attach it to a security container, it must be conspicuous and in close proximity to the security container.
- (d) Completed SF 702s must be maintained according to the NARA GRS 18.

- c. Combinations. Combinations must be classified and protected at the classification level and category of the matter being stored within the container. Control measures must be implemented to allow only a minimum number of people access to combinations for security containers. Combinations for containers containing ACREM must be limited to the responsible ACREM custodian and alternate ACREM custodian(s). When there are multiple shifts, the combination may be provided to an ACREM custodian and alternate ACREM custodian(s) for each shift. An individual designated as Emergency Notification

Personnel may be provided the combination only when the ACREM custodian and all alternate ACREM custodians are not available and access is required.

- (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) Initial receipt of a GSA-approved security container or lock.
 - (b) When an individual who knows the combination:
 - 1 is reassigned, transferred, or terminated;
 - 2 has his/her access authorization downgraded to a level lower than the level of classified matter stored;
 - 3 has his/her access authorization administratively terminated or suspended.
 - (c) Maintenance is performed by an uncleared locksmith or safe technician.
 - (d) When compromise or suspected compromise of a security container, its combination, or discovery of an unlocked and unattended security container containing classified matter is revealed.
 - (e) When the ACREM custodian(s) and/or alternate ACREM custodian(s) return after the combination has been provided to Emergency Notification Personnel in their absence.
 - (f) Preparation for turning in the container (the combination must be set to factory standard 50-25-50 before the container is turned in).

NOTE: Combinations used to protect communications security (COMSEC) material must be changed in accordance with DOE and National COMSEC requirements (see DOE M 200.1-1, *Telecommunications Security Manual*, dated 3-1-97, et al). Combinations used to protect North American Treaty Organization (NATO) material must be changed no less frequently than 12-month intervals.

- (2) Selection of Combination Settings. Combination numbers must be selected at random, avoiding simple ascending or descending series such as 10-20-30 or 50-40-30. Care also must be exercised to avoid selecting combinations of number that are easily associated with the person(s) selecting the combination (e.g., birth dates, anniversaries, social security number, or telephone extensions).

- (3) Protecting Combinations. To ensure proper protection of combinations, SF 700, part 2a (the record of the combination), must be marked and maintained as described above.
- (4) Identifying Personnel. In addition to the completion and maintenance of the SF 700 as described above, a record of all persons who know the combination also must be maintained.

CHAPTER II. CLASSIFIED MATTER PROTECTION AND CONTROL REQUIREMENTS

1. GENERAL. The protection requirements described in this chapter are consistent with the requirements set forth in the *National Industrial Security Program Operating Manual* (NISPOM). The Secretary of Defense acts as the Executive Agent of the National Industrial Security Program (NISP) and has final responsibility for issuing and maintaining the NISPOM. A copy of the NISPOM and all of its amendments can be found at <http://www.dss.mil/isec/nispom.htm>. Protection and control requirements include the following:
 - a. Classification level, category, and other information attributes listed in this Manual must be used in determining the protection and control required for 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 for the performance of official duties; access is not obtained by position only. Controls must be established to protect, deter, and detect unauthorized access to classified matter.
 - c. The originator of any matter that may be classified, including all matter that is prepared in a classified subject area, must ensure the matter is reviewed for classification by a derivative classifier. Prior to classification review, matter which may be classified must be protected at the highest potential classification level and category. Should any question exist regarding the classification of any draft documents or working paper, the originator is responsible for obtaining a classification review.
 - d. When information is prepared on classified information systems, hard-copy output (which includes paper, microfiche, film, and other media) must be marked either—
 - (1) as a final document 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 or
 - (2) as a working paper to the accreditation level and category of the information system (see Chapter II, Sections 3s and 4i 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 to produce consistent results. The following factors must be satisfied when exercising this option.

- (a) The output that will be produced must be fully defined and documented. The Designated Approving Authority 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 RD or FRD), and
- (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.

NOTE: The difference between option (1) and option (3), above is the time at which the classification review is conducted.

- e. 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 (see Figure II-1).
- f. Access to Classified Matter/Information in an Emergency. In an emergency involving an imminent threat to life or defense of the homeland, individuals who are not otherwise routinely eligible for access to classified matter or information may be granted access. Procedures must be developed for safeguarding classified matter in emergency situations. Local procedures must be developed describing the steps to be followed (i.e., notifications, alternative storage, and protection methods) in case of an emergency and approved by the Department of Energy (DOE) cognizant security authority.
 - (1) Access to Unsecured Classified Matter. If the emergency is life threatening (explosion, fire, etc.), the health and safety of individuals takes precedence over the need to secure classified matter. Therefore, emergency response personnel may require access to rooms where classified matter has not been properly secured. Local procedures must be developed instructing employees what to do (e.g., notifications, alternative storage and protection methods). The following actions must be taken at the time of the emergency:

TOP SECRET / SECRET / CONFIDENTIAL (Only When This Page is Filled-in and Appropriate Classification Indicated -- Circle One)	
Document Undergoing Classification Review Protect This Document At the Classification Level and Category Marked on This Page	
TO:	_____

FROM:	_____

DATE:	_____
<div style="border: 1px solid black; padding: 5px;"><p style="text-align: center;">RESTRICTED DATA</p><p>This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal Sanctions.</p></div>	<p style="text-align: center;">Instructions for Use of this Form (You do not need to be an Authorized Classifier to use this Form)</p> <ol style="list-style-type: none">1. Circle the highest estimated classification level at the top and bottom of this page (circle only one level).2. Circle the <i>Restricted Data</i> or <i>Formerly Restricted Data</i> Warning Notice (only if applicable). NOTE: <i>National Security Information</i> documents should have only the estimated classification level circled.3. Fill in "To," "From," and "Date" lines.4. Place this Form on top of the document pending classification review, and place an appropriate coversheet (SF-703 for Top Secret, SF-704 for Secret, or SF-705 for Confidential) on top of this page. <p><u>Note 1:</u> Document attached hereto may contain classified information and may or may not contain any classification markings. It must be protected as marked on this page. This cover page must remain with this document until a final classification determination has been made and the document has been appropriately marked by an Authorized Classifier.</p> <p><u>Note 2:</u> Top Secret documents must be hand carried or routed through an authorized courier. Use of any type mail or express mail service for Top Secret matter is prohibited. Transmittal of classified matter must be in accordance with DOE Orders.</p>
<div style="border: 1px solid black; padding: 5px;"><p style="text-align: center;">▲ Circle One (If Applicable) ▼</p><p>NOTE: <i>National Security Information</i> documents should have only the estimated classification level circled.</p></div>	
<div style="border: 1px solid black; padding: 5px;"><p style="text-align: center;">FORMERLY RESTRICTED DATA</p><p>Unauthorized Disclosure Subject to Administrative and Criminal Sanctions. Handle as Restricted Data in Foreign Dissemination. Section 144.b., Atomic Energy Act 1954.</p></div>	
TOP SECRET / SECRET / CONFIDENTIAL (Only When Attached to Potentially Classified Document and Appropriate Classification Indicated -- Circle One)	
<small>US Department of Energy, Washington, DC</small>	

Figure II-1 Cover Sheet for a Document Undergoing Classification Review

- (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) Security containers, vaults, and vault-type rooms (VTRs) must be inspected on return to the facility to ensure they have not been compromised.
- (2) Disclosure of Classified Information. An emergency situation may necessitate the intentional disclosure of classified information to individuals who are not otherwise eligible for access. If an emergency is life threatening (explosion, fire, etc.), 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 classified information concerning an improvised nuclear device found in a public place, sharing a classified 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. The following actions must be taken if such an intentional release is required:
- (a) Notification of Release. The following individuals must be notified as soon as possible of any emergency release of classified information to an individual or individuals who are otherwise not eligible for such access:
 - 1 for Restricted Data (RD) or Formerly Restricted Data (FRD), the Director, Office of Health, Safety and Security, and the Associate Administrator for Defense Nuclear Security, and
 - 2 for National Security Information (NSI), the appropriate DOE line management or DOE cognizant security authority.
 - (b) Protection Measures.
 - 1 The amount of classified information disclosed and the number of individuals to whom such information is disclosed must be limited to the absolute minimum to achieve the intended purpose.

- 2 The information must be transmitted over approved channels using the most secure and expeditious method.
- 3 A description of what specific information is classified and protection requirements for the information must be provided to the recipient.
- 4 A briefing must be provided to the recipient covering responsibilities about not disclosing the information, and a nondisclosure agreement must be signed by the recipient.
- 5 Physical custody of the information must remain with an authorized Federal Government entity in all but the most extraordinary circumstances.

(3) Reporting Requirements. Within 72 hours of access to unsecured classified matter or disclosure of classified information or the earliest opportunity that the emergency permits, but not later than 30 days after the release, the official making the disclosure decision must report the disclosure following the requirements and procedures for incidents of security concern (reference DOE M 470.4-1, *Safeguards and Security Program Planning and Management*) and must provide the office or agency with primary responsibility for the information with the following:

- (a) a description of the disclosed information;
- (b) a list of individuals to whom the information was disclosed;
- (c) a description of how the information was disclosed and transmitted;
- (d) the reason for the emergency release;
- (e) how the information is being protected; and
- (f) a description of briefings provided and a copy of the signed nondisclosure agreements.

2. CLASSIFIED MATTER IN USE. Classified matter in use must be constantly attended by, or under the control of, a person possessing the proper access authorization and need-to-know. When defense-in-depth exists, the DOE cognizant security authority may establish written local policy that allows classified matter to be left temporarily unattended during normal working hours within a locked room that is within an attended Limited Area (LA), Protected Area (PA), Material Access Area (MAA), or Exclusion Area (EA). The period of time must not exceed 1 hour. Locks must be individually coded or keyed and appropriate control measures implemented to mitigate the risk of unauthorized disclosure. The locking mechanism must be different than those used for routine protection of unclassified material or assets. Facilities must describe the

implementation of these protection measures in facility security plans. Classified automated information systems must be protected in a manner consistent with the approved security plan. This practice of leaving unattended classified matter unsecured for up to 1 hour will not be used as a routine method of protection. The practice of leaving unattended classified matter unsecured for up to 1 hour must not be used for special access program (SAP) information, sensitive compartmented information facilities (SCIFs), vaults, or vault-type rooms (VTRs).

3. MARKING. Classified matter marked according to previously published requirements need not be re-marked to conform with the following requirements, with the exception of paragraph 3.a.(1), which must be followed.

- 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). Documents must be marked in accordance with directives in place at the time of origin or later, or in accordance with current directives.
 - (a) If there is a question about the classification level or category of a document, the document must be reviewed by a derivative classifier and re-marked (if necessary) to clearly indicate the level and category and to ensure proper protection.
 - (b) Classified NSI documents that were created after April 1, 1996, and that lack appropriate current markings, including declassification on a date or event, classification authority, or classifier's name, should be reviewed by a derivative classifier to ensure the classification level and category are still correct and then remarked to bring them into conformance with current marking requirements. This must be done if the document is active, or is to be transmitted outside of the organization for other than official archiving purposes.
 - (c) Documents created before April 1, 1996, need only contain classification level and category (if RD or FRD) to ensure proper protection.
 - (d) Before using or distributing a document marked with the following obsolete markings, a derivative classifier or declassifier must determine the classification status and mark the document accordingly. DOE M 475.1-1A, *Identifying Classified Information*, provides requirements for reviewing and marking these documents. Pending review, documents must be handled and protected as Confidential/National Security Information (C/NSI).

- 1 Restricted. This is an obsolete U.S. classification marking used before December 15, 1953, that identifies a security level less sensitive than Confidential. This marking is still used by some foreign governments and international organizations.
- 2 Official Use Only (OUO). The Atomic Energy Commission used this term between July 18, 1949, and October 22, 1951, as an equivalent to the term Restricted. This marking is now used to identify unclassified information that may be exempt from disclosure under the Freedom of Information Act (FOIA).

(e) When possible, avoid returning documents because of improper markings. Instead, contact the sender and attempt to resolve any marking issues.

- (2) Markings. The following elements are common to all classified documents: classification level, classification category (if RD or FRD), caveats and/or special markings (if required), classifier information, originator identification, classification of titles or subjects, unique identification numbers (if in accountability), and portion marking (if NSI). The DOE Marking Handbook provides guidance and examples for marking classified documents. The originator is responsible for ensuring that each classified document is marked in accordance with this Manual.
- (3) Unique Identification Numbers. Classified matter required to be in accountability, as defined in paragraph 4. must have a unique identification number. To ensure control and accountability of this matter, the unique identification number must be placed on the first page of paper documents and on the top or front of non-paper documents. The first page of a document is the first sheet of paper (i.e., the cover page, title page, or first page of text).

b. Originating Organization and Date.

- (1) The name of the organization responsible for preparing the document and the date of preparation must appear on the first page of all classified documents. The first page of a document is the first sheet of paper, whether that is the cover page, title page, or first page of text.
- (2) Classified documents being taken offsite must be marked on the first page to show the mailing address of the organization responsible for preparing the document. The mailing address should consist of a street address or post office box, city, state, and zip code.

NOTE: When information in (1) and (2) cannot be accommodated on the first page, such as in the case of slides, microfiche, etc., this information must conspicuously accompany the classified document on a separate piece of paper (see 3.p. for instructions on marking special documents).

c. Classification Level.

- (1) The three classification levels, in descending order of sensitivity and potential damage to the National security, are Top Secret, Secret, and Confidential.
- (2) 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.
- (3) Each interior page of a classified document must be marked top and bottom with the highest classification level (or unclassified) of that page or the overall classification of the document.
- (4) Classification markings must be clearly distinguishable from the document text.
- (5) Classified material must have the classification level stamped, printed, etched, written, engraved, painted, or affixed to it by means of a tag, sticker, decal, or similar device. When marking is not practical, written notification of the markings must be furnished to recipients.
- (6) Blank interior pages of a classified document need not be marked with the classification level or category or the notice "This page intentionally left blank."

d. Classification Categories. The three classification categories are RD, FRD, and NSI. Classified documents containing only NSI need *not* be marked with the NSI category marking.

- (1) If the document is RD or FRD, 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 should appear in the lower left corner, as follows:

RESTRICTED DATA

This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure is subject to administrative and criminal sanctions.

FORMERLY RESTRICTED DATA

Unauthorized disclosure is subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination per Section 144.b, Atomic Energy Act, 1954.

- (2) Each interior page of a document containing RD or FRD must be marked top and bottom with the appropriate level and category of information on that page. If this is not feasible, the overall level and category of the document (if RD or FRD) may be applied to every page. For interior pages, the symbols RD and FRD may be used. These markings must be clearly distinguishable from the document text.
 - (3) Classified material (if RD or FRD) must have the classification category stamped, printed, etched, written, engraved, painted, or affixed to it by means of a tag, sticker, decal, or similar device. When marking is not practical, written notification of the markings must be furnished to recipients.
 - (4) RD or FRD documents generated prior to July 9, 1998, will not be required to be re-marked to indicate the category on each page containing RD or FRD information, unless they are sent outside the office of origin or holder for other than archiving purposes.
- e. Mixed Levels and Categories. DOE policy states that matter must be classified and marked at the highest level and category of the information contained in it. When classified matter contains a mix of information at various levels and categories that cause 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 access by an individual with a lower access level, such as an "L" cleared employee to be given access to a document that they might not otherwise have been authorized access to if the document was only marked at the highest overall classification level and category. (For example, a document that contains Confidential RD (C/RD) and Secret NSI (S/NSI) information would be required to be marked at the highest level and category, Secret RD (S/RD) in this case. None of the information in the document is S/RD.) However, this may not be interpreted to authorize any individual to gain access to information which exceeds their access authorization, 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. The derivative classifier's name and title are required only when a document is reviewed after

the initial classification determination has been made and the mixed level and category marking is applied. 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*

- f. Components. When components of a document are to be used separately, each major component must be 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 3.r., Transmittal Documents.
- g. 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 to be 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.
 - (3) Unclassified information must not be marked in a manner that would be confused with markings specified in this Manual for classified information (e.g., Confidential, etc.). If the unclassified matter carries a control marking [i.e., OUO, Unclassified Controlled Nuclear Information (UCNI), or Export Controlled Information (ECI)], the information must retain its control marking; it should not be re-marked unclassified.
- h. Portions.
- (1) For NSI documents, each section, part, paragraph, graphic, figure, or similar portion of any such document dated after April 1, 1997, must be marked to show the classification level or be identified as unclassified controlled information (e.g., UCNI, OUO) or as unclassified (U).

Classification levels of portions of a document must be shown by placing the appropriate classification symbol immediately following the portion's letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion.

- (2) Page changes to NSI documents dated after April 1, 1997, must be portion marked. Additionally, any NSI document that becomes active (i.e., sent outside the office of origin or holder other than for archival storage or removed from storage) must be portion marked with the appropriate classification level, unclassified controlled symbol (e.g., UCNI, OOU, etc.) or unclassified.
- (3) If any NSI document dated before April 1, 1997, is sent outside the office of origin or holder for other than archiving purposes, the entire document must be portion marked.
- (4) Documents containing RD or FRD are not required to be portion marked, however, in cases where portion markings are used, classification levels and categories (if RD or FRD) of portions of a document must be shown by placing the appropriate classification symbol immediately following the portion's letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion. Each section, part, paragraph graphic, figure, or similar portion of any such document must be accurately marked to show:
 - (a) the classification level and category (e.g., S/RD or S/FRD, C/FRD or C/FRD, S, TS, etc.);
 - (b) that it is unclassified controlled information (e.g., UCNI, OOU); or
 - (c) that it is unclassified (U).
- (5) Portion markings must include any applicable caveats (see 3.1. for information regarding caveats).
- (6) Portions of U.S. documents containing Foreign Government Information (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.

Classified documents generated by foreign governments do not require portion marking. Such documents generated and marked entirely by a foreign government must be protected commensurate with the level the foreign government specified.

- (7) Portions of U.S. documents containing North Atlantic Treaty Organization (NATO) information must indicate NATO or COSMIC (NATO Top

Secret documents), including the appropriate classification level (e.g., NATO-S or COSMIC-TS).

- (8) **Compilations.** In some instances, certain information that would otherwise be unclassified when standing alone may require classification when combined or associated with other unclassified information. When classification is required to protect a compilation of such information, the overall classification level and category (if RD or FRD) assigned to the document must be conspicuously marked or stamped at the top and bottom of each page, on the back of the last page of the document, and on the front cover, if any. A document classified for this reason is not required to be portion marked and must also contain the following statement on the first page: "This document has been classified under the compilation concept and shall not be used as the source for a derivative classification decision." The reason for classifying the information as a compilation also must be stated at an appropriate location near the beginning of the document.

i. Subjects and Titles.

- (1) Except for extraordinary circumstances, unclassified subject descriptors and titles must be used for classified documents because they are used on mail logs, document receipts, and other tracking or accountability records, most of which are entered into unclassified databases. Titles of classified documents must be marked, even if the document is not portion marked.
- (2) If subjects or titles are classified, they must be marked with the appropriate classification level, category (if RD or FRD), and any applicable caveats. If titles are not classified, they must be marked as unclassified or with the appropriate unclassified controlled marking (e.g., OUO).
- (3) The classification or control symbols (e.g., U, OUO, UCNI, C/RD, S/FRD) must be placed immediately after the title or subject.
- (4) When classified documents with unmarked titles and/or subjects become active (i.e., sent outside the office of origin or holder, or removed from storage), the titles and/or subjects must be reviewed by a derivative classifier and marked appropriately.
- (5) If a caveat (e.g., originator controlled (ORCON)) applies to the title or subject, it must be added to the title marking. A Secret NSI/ORCON title must be shown as S/ORCON.

j. Authorized Markings for Portions, Subjects, and Titles. The following are examples of the markings authorized for use with subjects and titles and when portion marking.

Unclassified: (U)

Official Use Only: (OUO)

Unclassified Controlled Nuclear Information: (UCNI)

Confidential National Security Information: (C)

Confidential Formerly Restricted Data: (C/FRD) or (CFRD)

Confidential Restricted Data: (C/RD) or (CRD)

Secret National Security Information: (S)

Secret Formerly Restricted Data: (S/FRD) or (SFRD)

Secret Restricted Data: (S/RD) or (SRD)

Top Secret National Security Information: (TS)

Top Secret Restricted Data: (TS/RD) or (TSRD)

Top Secret Formerly Restricted Data: (TS/FRD) or (TSFRD)

- k. Classifier Markings. Classifier marking requirements can be found in DOE M 475.1-1A.
- (1) Original Classification (NSI only). The following is an example of an original classifier marking.
- Classified by: (Name/personal identifier and position title)
- Reason: (NSI classification category)
- Declassify on: (Date or event)
- (2) Derivative Classification National Security Information (NSI).
- (a) Derivative Classifier Marking. The following is an example of an NSI derivative classifier marking.
- Classified by: (Name/personal identifier and position title)
- Derived from: (Title, date, agency, and where available, office of origin of guide/source document)
- Declassify on: (Date or event, and exemption category, when applicable)

- (b) The Originating Agency's Determination Required (OADR) Marking. The OADR marking is no longer authorized for new documents unless the new document is derived from an existing document that has OADR as the declassification date. This marking only applies to derivatively classified NSI documents. The following is an example of the use of the OADR marking on a new document.

Classified by: (Name/personal identifier and position title)

Derived from: (Guide/source document and date)

Declassify On: (Source marked "OADR")

- (3) Derivative Classification (RD and FRD). The following is an example of an RD and FRD classifier marking.

Classified by: (Name/personal identifier and position title)

Derived from: (Title, date, agency, and where available, office of origin of guide)

1. 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. Classified matter must be marked with caveats or special control markings, such as those indicated below, when required by Departmental directive or National policy. 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.

- (1) Caveats.

- (a) FGI. This caveat must be included on documents that contain information that is either classified or requires protection, and is received from a foreign government. Additional information on the marking, protection and control requirements for FGI are contained in paragraph 3.h.(6) and paragraph 9.

- (b) Director of Central Intelligence Information. The following markings, unless indicated otherwise, are authorized only for use for intelligence information:

- 1 No Foreign Dissemination (NOFORN). This marking indicates the information contained in the document may not be provided in any form to foreign governments,

international organizations, coalition partners, foreign nationals, or immigrant aliens without originator approval. This marking may be used for intelligence information and Naval Nuclear Propulsion Information (NNPI) only. (See paragraph 3l(5) for additional information regarding NNPI)

- 2 ORCON. This marking indicates the document bearing the marking is controlled by the originator. Reproduction of, extraction of information from, or redistribution of such a document requires the permission of the originator. This marking must be used only on classified documents containing intelligence information that clearly identifies or would reasonably permit the identification of intelligence sources or methods. It must not be used when access to the information can be reasonably protected by its classification markings or any other control markings.

Without advanced permission from the originator, the dissemination of ORCON beyond the DOE Headquarters intelligence components and the formally designated field intelligence elements is limited. As a condition for receipt of ORCON by a non-intelligence component, written assurance that the recipient will observe the provisions of the Director of Central Intelligence Directive must be provided to the Office of Intelligence.

- 3 Proprietary Information (PROPIN). This marking indicates the information contained in the document must not be released outside the Federal Government in any form to an individual, organization, or foreign government that has any interests, actual or potential, in competition with the source of the information without the permission of the originator of the intelligence information and provider of the proprietary information. This precludes dissemination to contractors, irrespective of their status within the Government, without the above consent.

- 4 Authorized for Release to Country (REL TO). This marking applies to intelligence information the originator has predetermined to be releasable or has released through established foreign disclosure procedures and channels to specified foreign countries or international organizations. The name of country or countries authorized access to the document must be included after the caveat (e.g., REL TO Canada, United Kingdom, etc.). The name of the country may be spelled out or abbreviated, but must be identifiable.

- 5 Releasable by Information Disclosure Official (RELIDO). RELIDO is a dissemination marking that may be applied to intelligence information to indicate that the originator has authorized Designated Intelligence Disclosures Officials (DIDO) to make further sharing decisions in accordance with the existing procedures for uncaveated intelligence material (intelligence with no restrictive dissemination controls). RELIDO may be used independently or in conjunction with the “REL TO” dissemination marking (e.g., Secret//RELIDO or SECRET//REL TO USA, AUS, GBR/RELIDO).
- 6 Obsolete Markings. The following markings are no longer used, but remain applicable on the documents that bear these markings until such time as the document is re-reviewed and re-marked:
- a No Dissemination to Contractors (NOCONTRACT).
 - b Warning Notice Intelligence Sources and Methods (WNINTEL). NOTE: Existing instances of these markings remain valid until the documents containing them are re-reviewed and re-marked for classification purposes, or until they become declassified.

(2) Special Control Markings.

- (a) NATO Information. Individuals must have received special access approval by the DOE NATO Sub-registry or the local DOE NATO Control Point to be eligible for access to NATO information.

- 1 NATO Security classifications indicate the sensitivity of NATO information and are applied in order to alert recipients to the need to ensure protection in proportion to the degree of damage that would occur from unauthorized access or disclosure. NATO security classifications and their significance are:
- a COSMIC TOP SECRET (CTS) unauthorized disclosure would result in exceptionally grave damage to NATO.

- b NATO SECRET (NS) unauthorized disclosure would result in grave damage to NATO.
- c NATO CONFIDENTIAL (NC) unauthorized disclosure would be damaging to NATO.
- d NATO RESTRICTED (NR) unauthorized disclosure would be detrimental to the interests or effectiveness of NATO.

2 NATO UNCLASSIFIED. By definition UNCLASSIFIED is not a security grading, therefore, NATO UNCLASSIFIED information is not subject to the security procedures which cover the control of information classified NATO RESTRICTED or above. However, all NATO information, whether classified or unclassified, which is released to another Party is for official use only; therefore, unclassified NATO information must always be marked NATO UNCLASSIFIED, and may only be disseminated to bodies and individuals with a need-to-know. Access to this information by non-NATO entities is permitted when such access would not be detrimental to NATO. In this regard, it is similar to U.S. Government official information that must be reviewed prior to public release. Additionally, any administrative markings placed on NATO UNCLASSIFIED (e.g., in confidence, commercially sensitive) indicate sensitivity of the information.

(3) Qualifying Markings.

- (a) NATO marking. The marking NATO is applied to all information (except those marked COSMIC TOP SECRET), including ATOMAL, prepared for circulation within NATO. The markings NATO and COSMIC signify that the information must not be passed outside the North Atlantic Treaty Organization except by the originator, or with the originator's consent.
- (b) COSMIC marking. COSMIC is a NATO marking and designation which is synonymous with TOP SECRET information and is applied exclusively to TOP SECRET material prepared for circulation within NATO.
- (c) NATO also has markings to identify Special Category Information to which additional handling/protection procedures, not covered by the core NATO policy document, are applied. Special Category Information and their NATO markings include:

- 1 ATOMAL is a NATO marking applied to special category information signifying that the information shall be protected in accordance with the Agreement Between the Parties to the North Atlantic Treaty for Cooperation Regarding Atomic Information, [C-M(64)39, dated June 18, 1964], and the latest version of C-M(68)41, Administrative Arrangements to Implement the agreement Between the Parties to the North Atlantic Treaty for Cooperation Regarding ATOMAL Information, which implements the Agreement and sets forth procedures, functions, and responsibilities of NATO components for handling and protecting ATOMAL information. This [i.e., ATOMAL], special category information is either U.S. Atomic information (RD or FRD) or United Kingdom Atomic information. Documents containing ATOMAL information communicated under the Agreement for Cooperation Regarding ATOMIC Information C-M(64)39 first bear the NATO marking, followed by the applicable security classification in accordance with its original classification and content, followed by the word ATOMAL.
- 2 U.S. Single Integrated Operations Plan (US-SIOP) is a marking applied to special category information signifying that the information shall be protected in accordance with C-M(71)27(Revised), Special Procedures for the Handling of U.S. Single Integrated Operational Plan (US-SIOP) Information Within NATO, dated November 23, 1979. US-SIOP documents which do not contain ATOMAL information will be classified COSMIC TOP SECRET, NATO SECRET, or NATO CONFIDENTIAL in conformance with its original classification and content, in addition to the US-SIOP marking. US-SIOP information is not classified NATO RESTRICTED or NATO UNCLASSIFIED. Documents that contain ATOMAL information will be classified COSMIC TOP SECRET ATOMAL, NATO SECRET ATOMAL, or NATO CONFIDENTIAL ATOMAL in conformance with its original classification and content, in addition to the US-SIOP marking.
- 3 The term CRYPTO is a NATO marking and a special category designator identifying all COMSEC keying material used to protect or authenticate telecommunications carrying NATO security-related information. It signifies

that the information shall be protected in accordance with the appropriate cryptographic security instruction.

- (d) **Dissemination Limitation Markings.** As an additional marking to further limit the dissemination of NATO classified and unclassified information, a Dissemination Limitation Marking may be applied by the originator.
 - (e) **Assignment of Classification Responsibility.** The responsibility for determining whether official information should be marked NATO UNCLASSIFIED or be given a particular level of security classification rests exclusively with the originating member nation or NATO command or agency. Questions concerning NATO information must be directed to the DOE NATO Sub-registry within the Office of Health, Safety and Security or DOE NATO Control Point or the Office of Classification and Information Control.
- (4) **Weapon Data.** The following markings are associated with atomic weapons or nuclear explosive devices and are placed on the first page [cover sheet (if any), title page (if any) or first page of text]:
- (a) **Sigma Category.** This marking refers to RD and FRD specifically defined in 12 separate categories (1-5 and 9-15) concerning the design manufacture, or use of atomic weapons or nuclear explosive devices. The use of the term Sensitive Use Control Information (SUCI) has been eliminated. This information is now defined as Sigma 14 and Sigma 15 information. Sigmas are marked as “SIGMA #”, with # being the relevant sigma number.
 - (b) **Critical Nuclear Weapons Design Information (CNWDI).** This is a Department of Defense marking designating Top Secret or S/RD that reveals the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munition, or test device. For more details, refer to DOE 5610.2, *Control of Weapons Data*, dated August 1, 1980.
- (5) **Naval Nuclear Propulsion Information (NNPI).** This is a type of information (classified or unclassified) concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, or repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated nuclear support facilities. Classified and unclassified NNPI must be protected in accordance with Naval Sea Systems Command Instruction C5511.32B, dated 12-22-93. NNPI must be protected pursuant to export control requirements and statutes. Questions regarding NNPI must be directed to the Deputy Administrator for Naval Reactors.

- (a) Access to NNPI must be granted only to U.S. citizens who have a need-to-know and, if classified NNPI, the recipient must also have the proper access authorization.
- (b) Both classified and unclassified NNPI documents are designated as NNPI by being marked as follows:
 - 1 NOFORN. This document is subject to special export controls and each transmittal to foreign governments or foreign nationals must be made only with the prior approval of Naval Sea Systems Command (this marking should be placed on the bottom of the first page of text).
 - 2 All subsequent pages must be marked top and bottom NOFORN.

NOTE: The use of NOFORN for NNPI is the only situation in which intelligence caveats may be used for marking documents that are not intelligence related.

- (6) Special Category (SPECAT). This is a program controlled by the Department of Defense that generally operates at the Secret level. SPECAT is neither a code word or a SAP. SPECAT programs use focal point control officers (FPCOs) to control the dissemination and handling of NSI contained within the program. There are a number of SPECAT programs in DOE. The NNSA is the DOE primary FPCO for SPECAT and should be contacted for additional information regarding the program.
- (7) Dissemination and Reproduction Notices. When programmatic requirements place special dissemination or reproduction limitations on classified information, one of the following notations, or one similar in content, must be used:
 - (a) FURTHER DISSEMINATION ONLY AS AUTHORIZED BY GOVERNMENT AGENCY.
 - 1 This notation applies to documents whose further dissemination within the receiving facility is restricted to persons authorized by the addressee.
 - 2 Dissemination outside the facility is prohibited without the approval of the originating agency.
 - (b) REPRODUCTION REQUIRES APPROVAL OF ORIGINATOR. This notation applies to documents that must not be reproduced without specific, written approval of the originator.

- m. Remarking Upgraded, Downgraded, and Declassified Matter. When an official upgrade, downgrade, or declassification notice is received, the initial classification markings must be stricken and replaced with the new classification markings. The authority for and date of the upgrading, downgrading, or declassification notice must be entered on the first page of the document. The originator or document custodian must notify all known holders of the document.
- (1) General. Refer all upgrading, downgrading, and declassification issues to the local classification office. For details, see DOE M 475.1-1A, *Identifying Classified Information*, dated 2-26-01.
 - (2) Record Retention. The original change notice is considered record material and must be retained in accordance with National Archives Records Administration (NARA) General Records Schedule (GRS) 18.
 - (3) Historical Document Review Markings. See Table II-1 for approved NSI classification markings when completing historical document reviews.
 - (4) Upgrading. A derivative classifier may upgrade the classification of a document or material within his/her designated authority. The custodian of a document or material may upgrade its classification markings upon receipt of an upgrade notice from the proper authority. The originator or document custodian must notify all known holders with the proper access authorization when a document has been upgraded. Upon receipt of the authorization to upgrade a classified document, the first page of the document must be marked to show the:
 - (a) date the classified document was upgraded;
 - (b) authority for upgrading the document (e.g., a memorandum, an Office of Scientific and Technical Information notice).

Example of upgrade marking:

Classification Upgraded: (Insert date document was upgraded)
Upgrade Authority: (Authority for change in classification)

- (5) Downgrading. A derivative declassifier may downgrade the classification of a document or material within his/her designated authority. The custodian of a document or material may downgrade its classification markings upon receipt of a downgrade notice from the proper authority. When the authorization to downgrade a classified document is received, the first page of the document must be marked to show the:
 - (a) date the classified document was downgraded; and

Table II-1. National Security Information Historical Document Review Markings

MARKING	EXPLANATION
<p><u>CLASSIFICATION RETAINED</u> DOE NSI DECLASSIFICATION REVIEW EXECUTIVE ORDER 12958, as amended, EXEMPTION/RETENTION BY CG-HR-1 TOPICS: BY (NAME/ORGANIZATION):</p>	<p>This stamp would be used when reviewing a DOE or other agency NSI classified document that contains DOE classified information exempt from automatic declassification.</p>
<p><u>CLASSIFICATION CANCELED</u> DOE NSI DECLASSIFICATION REVIEW EXECUTIVE ORDER 12958, as amended, BY (NAME/ORGANIZATION):</p>	<p>This stamp would be used when reviewing a DOE NSI classified document that no longer contains DOE or other agency classified information.</p>
<p><u>CONTAINS NO DOE CLASSIFIED INFO</u> DOE NSI DECLASSIFICATION REVIEW EXECUTIVE ORDER 12958, as amended, BY (NAME/ORGANIZATION):</p>	<p>This stamp would be used when reviewing another agency document that the review confirmed contained no DOE classified information.</p>
<p><u>CONTAINS NO DOE CLASSIFIED INFO</u> COORDINATE WITH: DOE NSI DECLASSIFICATION REVIEW EXECUTIVE ORDER 12958, as amended, BY (NAME/ORGANIZATION):</p>	<p>This stamp would be used when reviewing a DOE NSI classified document that no longer contains agency classified information but may contain other agency classified information. The agency's name would be entered on the "coordinate with" line.</p>
<p><u>CONFIRMED TO BE UNCLASSIFIED</u> DOE NSI DECLASSIFICATION REVIEW EXECUTIVE ORDER 12958, as amended, BY (NAME/ORGANIZATION):</p>	<p>This stamp would be used when reviewing a DOE purportedly unclassified document that is confirmed to contain no currently classified information.</p>
<p>WITH ATTACHMENTS/ENCL</p>	<p>This stamp would be used when reviewing a document that had attachments or enclosures to confirm that the attachments or enclosures were also reviewed. It would be placed just above or below the review stamp to emphasize that the review applies to the attachments/ enclosures.</p>
<p>WITHOUT ATTACHMENTS/ENCL</p>	<p>This stamp would be used when reviewing a document that indicated it had attachments or enclosures but the attachments or enclosures were not reviewed. It would be placed just above or below the review stamp to emphasize the review did not apply to the attachments/ enclosures.</p>
<p>THIS PAGE ONLY</p>	<p>This stamp would be used to indicate that the review was conducted only on a single page (e.g., one page separated from a multi-page document).</p>

- (b) authority for downgrading the document (e.g., a memorandum, an Office of Scientific and Technical Information notice).

Example of downgrade marking:

Classification Downgraded: (Insert date document was downgraded)

Downgrade Authority: (Authority for change in classification).

- (6) Declassifying. When the authorization to declassify a classified document is received, the classification markings must be crossed out, the term “Unclassified” must be substituted, and the following information must be applied to the first page of the document (unless unclassified controlled information is involved, which is addressed in paragraph n., below):

- (a) the names/personal identifiers and position titles of individuals declassifying the document;
- (b) the designation of the guidance used as the basis for the declassification determination and the dates of such documents are entered on the “Derived from” line, or authority for declassifying the document (e.g., a referenced memorandum, an Office of Scientific and Technical Information notice, etc.); and
- (c) the date of declassification.

Example of declassification marking.

Declassified by: (Name/personal identifiers and position titles)

Derived from: (Designation of guidance or source document and date of such document, or authority for declassifying the document.)

Declassified on: (Date of declassification)

- n. Remarking Automatically Declassified Matter. Matter marked for automatic declassification may be declassified and remarked accordingly on the date or event identified for declassification. Matter not marked for automatic declassification will remain classified until the originating agency makes a determination. Matter that is marked with downgrading or declassification instructions must be remarked to comply with the instructions on the matter. However, even after matter is declassified, it may still require protection based on other requirements (e.g., OOU information, UCNI, Protected Critical Infrastructure Information [PCII], etc.).

- o. Classified Matter Not Automatically Declassified. See DOE M 475.1-1A for these requirements.
- p. Marking Special Documents. Unless otherwise stated, standard marking requirements remain in effect. The following are requirements for marking special documents.
 - (1) Charts, Maps, Drawings, and Tracings. When such documents are printed on larger than the standard 8.5-inch by 11-inch sheets, the overall level and category (if RD or FRD) of the document must be marked under the legend, title, or scale block. The classification level and category (if RD or FRD) must be visible when these types of documents are folded or rolled. These types of NSI documents do not require portion marking unless such markings are determined by the cognizant classification or security authority to be operationally necessary. The unique identification number, if accountable, should be placed either in the upper, right-hand corner or under the legend, title, or scale block. If the chart, map, or drawing is incorporated into a document, it will be marked the same as any other page of the document.
 - (2) Messages. The overall classification level and category (if RD or FRD) of the message must be the first item of information in the text. When messages are printed by an automated system, markings may be applied by that system provided the markings are clearly distinguishable from the informational text. If applicable, declassification instructions must be included on the last line of text and may be abbreviated as DECL (date, exemption, or event).
 - (3) Classified Electronic Mail (E-Mail) Messages.
 - (a) General.
 - 1 Classified e-mail messages must be transmitted only on systems approved for classified transmissions and in accordance with the system security plan.
 - 2 Classified e-mail must be sent only to individuals with an appropriate access authorization, any required formal access approval, and need-to-know.
 - 3 Final documents, resulting from e-mail messages, including attachments, require classification marking as specified in this Manual.
 - 4 Classified e-mail messages that meet the definition of Federal records (ref. GRS as issued by the Archivist of the

United States) are subjected to record retention requirements.

(b) Marking of Classified E-Mail Messages.

- 1 Each classified e-mail message must include:
 - a As the first item of information in the text, the highest level and category of the accredited classified information system or the appropriate markings for the classification of the information as determined by a derivative classifier;
 - b Name and organization of originator;
 - c Date of transmission;
 - d Subject and title marking as required for all classified documents (see paragraph 3.i., Subjects and Titles); and
 - e Any applicable caveats or special handling and dissemination requirements.
- 2 Any attachment to a classified e-mail message must be appropriately marked:
 - a At the top and bottom of each page with the highest level and category of the accredited classified information system; or
 - b As a final document with the appropriate classification of the information as determined by a derivative classifier.
- 3 If the e-mail message or attachment is printed to hard copy, the recipient must ensure it is marked appropriately, either:
 - a As a working paper, or
 - b As a final document by obtaining a classification review by a derivative classifier or, if a derivative classifier is not available at the recipient's location, by having the originator provide a message already reviewed by a derivative classifier and marked in final format.

- 4 A hard copy of a classified e-mail message or attachment that was marked as a working paper when printed must be marked as final when:
 - a Distributed outside the recipient's immediate organization (e.g., division, section, or team) or ad hoc working group² (AHWG) by any means, or
 - b Retained for more than 180 days, or
 - c Filed permanently.
- (c) Electronic Distribution of Classified Documents.
 - 1 When electronic means are used to distribute a classified document outside the sender's immediate organization (e.g., division, section, or team) or AHWG, the sender must ensure the document is marked as a final document.
 - 2 The recipient must verify that any printed copies contain appropriately applied markings, must mark the back of the last page of each document with its classification level and category (if RD or FRD), and must attach appropriate cover sheets.
- (d) Unclassified E-mail Messages.
 - 1 The first line of an unclassified e-mail message without classified attachments sent on a classified e-mail system must indicate the message is unclassified. If the e-mail contains unclassified controlled information, it must retain its unclassified control marking.
 - 2 Unclassified e-mail messages containing classified attachments must indicate the overall classification level, category (if RD or FRD), and applicable caveats associated with each attachment. The classified attachments must contain the classification markings required for a final document.
 - 3 The recipient is responsible for applying the appropriate classification markings (e.g., ensuring that level, and

² An AHWG is a formally defined group of individuals participating in a specific activity or project or group of activities or projects in which all members have been determined to have the appropriate access authorization, any required formal access approvals, and need-to-know. The AHWG must have the ability to limit access to on-line activities to only those members of the AHWG and use that ability when transmitting classified information which is not marked as a final document as determined by a derivative classifier.

category if RD or FRD, is placed on the top and bottom on every page and the back of the final page) if the message and/or attachment is printed in hardcopy at the receiving location.

- (4) Facsimiles. A classified document transmitted by an approved classified facsimile machine must be marked, if possible, as a final document before transmission. DOE F 1325.7, Telecommunication Message, may be used as the first page of the facsimile. This form or a locally developed form may be marked either as an unclassified letter of transmittal or as the first page of the classified document (see Figures II-2a and II-2b). When classified drafts are transmitted by facsimile, they should be marked at the highest potential overall classification level and category. When final classification determination is made, the originating agency is responsible for ensuring that all previous recipients receive a correctly marked version with instructions to destroy all previous draft copies.
- (5) Microforms.
- (a) General.
- 1 Microforms contain images or text in sizes too small to be read by the unaided eye. Classification and category markings must consider the media involved but must be readable by the unaided eye.
 - 2 All required markings must be on the individual documents contained on the microforms.
 - 3 All microforms must contain markings specified by this Chapter (with the exception of classifier, classification guide, and declassification information) on the medium (e.g., microfiche or reel).
 - 4 All documents placed on classified microforms must be specifically identified as being either classified or unclassified.
 - 5 Microforms created before July 15, 1994, do not need to be redone if the documents contained on them are not individually marked as independent documents.
- (b) Microfiche. Each microfiche must be marked either photographically on the film or by using an adhesive label.
- 1 The first and last image of each microfiche should reflect the highest classification level, category (if RD or FRD),

DOE F 1325.7
(03-98)
(Exception to SF 14, Approved by NARS, June 1978)

INSTRUCTIONS

(NOTE: More detailed requirements and instructions are contained in DOE M 471.2-1A and DOE 5300.1C.

1. **and 15. Classification:** If the message is classified, stamp the overall classification level in the designated area at the top and bottom of the form.
2. **Message Contains Weapon Data:** The originator shall mark the appropriate block either "YES" or "NO", otherwise the message center will not transmit the message.
3. **Page Count:** Insert the total number of pages being transmitted.
4. **Precedence Designation:** High precedences are reserved for use only under specified conditions. Average transmission times exclusive of messenger services are shown. Messages having undesignated precedences are sent as "Routine."
5. **Type of Message:** Self-explanatory.
6. **From:** Type name of organization on the first line, the name and routing symbol of the sender on the second line, and the city and state on the third line.
7. **Signature of Authorizing Official:** The official authorized to certify the message as "Official Business" signs here. The time should be added to the signature block as a means of establishing the in date time group for use in future replies or inquiries to the message.
8. **Date:** Insert the date the message is signed for dispatch.
9. **To:** Place each address on one line if possible. If more than one addressee, double space between each. List information addressees in the address portion of the message if electrical transmission is required or if you wish the other addressees to know they are being furnished a copy. Send information copies by mail whenever possible. To indicate that electrical transmission is not required, place the letters "ZEN" before the action or information address. The originator is responsible for transmitting these copies.

Message Text: Start the body of the message three spaces below the address and double space between lines. Use block style. Be brief, use coined words, commonly understood abbreviations, ordinary punctuation, and numerals. Omit the articles "a", "an," and "the" unless needed for clarity or part of a quoted passage. Limit each line of text to 69 characters and spaces (note margin guides).

Continuation Pages: Use plain paper.
10. **Originator:** Type the name of the originator, initials of the typist, the telephone number, and the routing symbol of the originating organization.
11. **through 14.** Choose the appropriate classifier marking and complete the required information.

Figure II-2b. DOE F 1325.7, Telecommunication Message Instructions

and caveats (if applicable) of information contained on the microfiche.

2 Declassification instructions³ (NSI only) should be placed on the microfiche so it is readable with the unaided eye, if such marking would apply to all of the classified information on the microfiche. If it will not fit, the declassification instructions should be placed on accompanying documentation.

3 The classification level and category (if RD or FRD) and unique identification number (if accountable) must be placed across the top of the microfiche. The classification level and category (if RD or FRD) must also be placed on the bottom (classification level and category must be readable by the unaided eye).

(c) Microfilm. Each microfilm reel must be marked on its face (i.e., on the reel itself) to reflect the classification level, category (if RD or FRD), caveats (if applicable) and unique identification number (if accountable). Declassification instructions must be placed on the reel, if such markings would apply to all the classified documents on the microfilm. If these instructions will not fit, they must accompany the microfilm (consider placing this information on accompanying documentation) (see Figure II-3).

1 Declassification instructions must be placed on the first image, *if* such instructions would apply to *all* the classified documents on the microfilm. If the instructions will not fit, they must be placed on accompanying documentation.

2 The second image should contain the reel number.

3 The third image should contain the reduction ratio used in microfilming the documents.

4 The image immediately preceding the end of the reel should contain an index of the documents microfilmed.

5 The end of each reel must contain the highest level and category (if RD or FRD) of information on the reel.

³ Historical documents may have downgrading instructions instead of declassification instructions. Downgrading instructions are obsolete markings.

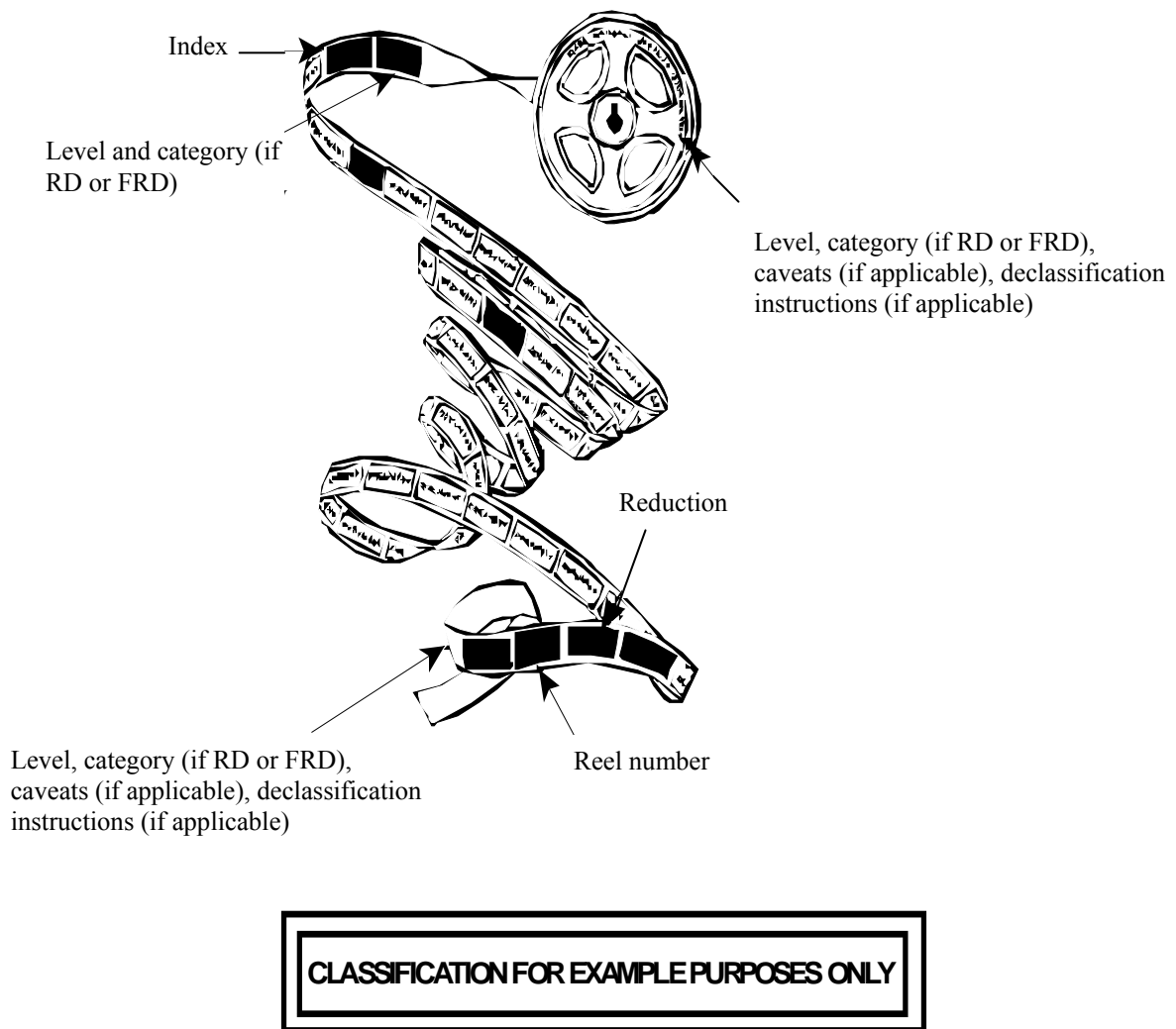


Figure II-3. Example Markings for a Classified Microfilm Reel

- (6) Motion Picture Films or Video Tapes. At the beginning of a film or video tape, the following information must be projected for approximately 5 seconds in the sequence given: classification level, classification category (if RD or FRD), caveats (if applicable), classifier information, and unique identification number (if accountable). At the end of a film or videotape, the classification level and category (if RD or FRD) must be projected for approximately 3 seconds. The face of the video tape cartridge or the face/side of the film's reel must be marked with the classification level and category (if RD or FRD).

Only the *removable* covering of a film or tape is considered a container and must be marked according to other containers (paragraph 3.q).

(7) Photographs. Classification markings (classification level, category [if RD or FRD], caveats [if applicable], classifier information, and the unique identification number, if accountable) must be applied (if necessary, to the reverse side or affixed by a pressure tape label, staple strip, or other comparable means). When self-processing film or paper is used to photograph or reproduce classified information and all parts of the last exposure have not been removed from the camera, the camera must be protected at the highest classification level and category of information contained on the medium.

(8) Negative Rolls. Roll negatives or positives must be marked at the beginning and end of each strip. The markings at the beginning of a roll must be placed in the following order: classification level, category (if RD or FRD), caveats (if applicable), classifier information, and the unique identification number (if accountable). The markings at the end of the roll must have the classification level and category (if RD or FRD)

NOTE: Any rolls created prior to publication of this Manual may be marked according to the marking requirements in place at the time the roll was originated. Copies of such previously created rolls must be marked according to current requirements.

(9) Transparencies, Slides, and Sheet Film.

(a) The overall classification level, category (if RD or FRD), and any caveats must be shown on the image of the first transparency, slide, or sheet film of a series. All other applicable markings specified in this chapter must be shown on the border or the frame or in the accompanying documentation. The succeeding transparencies, slides, and sheet film must indicate the classification level and category (if RD or FRD) on the image.

(b) When individual pages in a set of transparencies, slides, or sheet film are to be handled and controlled as separate documents, each page requires all standard markings.

(c) Each transparency, slide, or sheet film may be regarded as an individual portion and does not require further portion marking.

(10) Recordings. Magnetic, electronic, or sound recordings must indicate the overall classification level, category (if RD or FRD), and applicable caveats at the beginning and end of the recording. The classification level, category (if RD or FRD), caveats (if applicable), unique identification number (if accountable), and classifier information must be applied to the face of the recording by adhesive tape or similar material.

- (11) Classified Information Systems Media. All classified information systems media must be marked with the accreditation level of the information system unless an appropriate classification review has been conducted. All classified electronic storage media (ESM) must have the overall classification level and category (if RD or FRD) visible on the front and back. Media may be marked using a standard form (SF 710 for unclassified, SF 709 for classified, SF 708 for Confidential, SF 707 for Secret, and SF 706 for Top Secret (see <http://www.archives.gov/isoo/security-forms/>) or locally developed labels containing the information on the SFs. Classifier markings are not required on the exterior of ESM. Only the *removable* covering of classified ESM is considered a container and must be marked according to paragraph 3.q.
- (a) If a platen or disk is removed from its manufacture’s case and is not immediately destroyed, it must be marked with the classification level and category (if RD or FRD).
 - (b) Labels that denote the classification level and category (if RD or FRD) of the media may be used when it is practical to apply the label without impeding the operation of the removable media.
 - (c) If the label can impede the operation of the removable media, (e.g., not allowing the media to properly seat), alternative marking methods are required.
 - (d) The classification markings must be visible and human-readable, and must easily communicate the classification level and category (if RD or FRD) of the information.
- (12) Translations. U.S. classified information translated into a foreign language must be marked as U.S. classified information and must show the equivalent foreign government classification (see Table II-2).

Table II-2. Foreign Equivalent Classification Markings

Country	Top Secret	Secret	Confidential	Confidential FGI-Modified Handling Authorized*
Argentina	Estrictamente Secreto	Secreto	Confidencial	Reservado
Australia	Top Secret	Secret	Confidential	Restricted
Austria	Streng Geheim	Geheim	Verschluss	
Belgium (Flemish)	Zeer Geheim	Geheim	Vertrouwelijk	Bepertke Verspreiding

* Provided that this level of protection is at least equivalent to that provided by the foreign government, but less than U.S. Confidential.

Table II-2. Foreign Equivalent Classification Markings (continued)*

Country	Top Secret	Secret	Confidential	Confidential FGI-Modified Handling Authorized*
Bolivia	Supersecreto or Muy Secreto	Secreto	Confidencial	Reservado
Brazil	Ultra Secreto	Secreto	Confidencial	Reservado
Cambodia	Sam Ngat Bamphot	Sam Ngat	Roeng Art Kambang	Ham Kom Psay
Canada	Top Secret	Secret	Confidential	Restricted
Chile	Secreto	Secreto	Reservado	Reservado
Columbia	Ultrasecreto	Secreto	Reservado	Confidential Restringido
Costa Rica	Alto Secreto	Secreto	Confidencial	
Denmark	Yderst Hemmeligt	Hemmeligt	Fortroligt	Tiltjenestebrug
Ecuador	Secretisimo	Secreto	Confidencial	Reservado
El Salvador	Ultra Secreto	Secreto	Confidencial	Reservado
Ethiopia	Yemiaz Birtou Mistir	Mistir	Kilkil	
Finland	Erittain Salainen	Salainen		
France	Tres Secret	Secret Defense	Confidentiel Defense	Diffusion Restreinte
Germany	Streng Geheim	Geheim	Vs-Vertraulich	
Greece	AKPΩΣ AΠOΠΠITON	AΠOΠΠITON	EMΠIΣTEYTI KON	ΠEΠIΩΠIEMENHΣ XΠHΣEΩΣ
Guatemala	Alto Secreto	Secreto	Confidencial	Reservado
Haiti	Top Secret	Secret	Confidential	Reserve
Honduras	Super Secreto	Secreto	Confidencial	Reservado
Hong Kong	Top Secret	Secret	Confidential	Restricted
Hungary	Szigoruan Titkos	Titkos	Bizalmas	
Iceland	Algjorti	Trunadarmal		
India	Param Gupt	Gupt	Gopniya	Pratibanhst/seemit
Indonesia	Sangat Rahasia	Rahasia	Agak Rahahasia	Terbatas
Iran	Bekoliserri	Serri	Kheil Mahramaneh	Mahramaneh
Iraq	Sirri Lil-ghaxah	Sirri	Khass	Mehdoud
Ireland (Gaelic)	An-sicreideach	Sicreideach	Runda	Srianta
Israel	Sodi Beyoter	Sodi	Shamur	Mugbal
Italy	Segretissimo or Segretissimo	Segreto	Riservatissimo	Riservato
Japan	Kimitsu	Gokuhi	Hi	Toriatsukaichui
Jordan	Maktum Jiddan	Maktum	Sirri	Mahdud
Korea	I-Kup Bi Mil	II-Kup Bi Mil	III-Kup Bi Mil	Bu Woi Bi

* Provided that this level of protection is at least equivalent to that provided by the foreign government, but less than U.S. Confidential.

Table II-2. Foreign Equivalent Classification Markings (continued)*

Country	Top Secret	Secret	Confidential	Confidential FGI-Modified Handling Authorized*
Laos	Lup Sood Gnod	Kuam Lup	Kuam Lap	Chum Kut Kon Arn
Lebanon	Tres Secret	Secret	Confidential	
Mexico	Alto Secreto	Secreto	Confidencial	Restringido
Netherlands	Zeer Geheim	Geheim	Confidentieel or Vertrouwelijk	Dienstgeheim
New Zealand	Top Secret	Secret	Confidential	Restricted
Nicaragua	Alto Secreto	Secreto	Confidencial	Reservado
Norway	Strengt Hemmelig	Hemmelig	Konfidensiell	Begrenset
Paraguay	Secreto	Secreto	Confidencial	Reservado
Pakistan (Urdu)	Intahai Khufia	Khufia	Sigha-E-Raz	Barai Mahdud Taqsim
Peru	Estrictamente	Secreto	Secreto Confidencial	Reservado
Philippines	Top Secret	Secret	Confidential	Restricted
Portugal	Muito	Secreto	Secreto Confidencial	Reservado
Saudi Arabia	Saudi Top Secret	Saudi Very Secret	Saudi Secret	Saudi Restricted
Spain	Maximo Secreto	Secreto Confidencial	Diffusion Limitada	
Sweden (Red Borders)	Hemli	Hemli		
Switzerland	(Three Languages: French, German and Italian. TOP SECRET has a registration number to distinguish from SECRET and CONFIDENTIAL.)			
Taiwan	Chichimi	Chimi		
Thailand	Lup Tisud	Lup Maag	Lup	Pok Pik
Turkey	Cok Gizli	Gizli	Ozel	Hizmete Ozel
Union of South Africa (English)	Top Secret	Secret	Confidential	Restricted
Afrikaans	Uiters Geheim	Geheim	Vertroulik	Beperk
United Arab Republic Egypt	Jirri Lilghaxeh	Sirri	Khas	Mehoud Jidden
United Kingdom	Top Secret	Secret	Confidential	Restricted
Uruguay	Ultra Secreto	Secreto	Cofidencial	Reservado
Russia	Совершенно Секретно	Секретно	Не Подлежащий Оглашению	Для Служебного Пользования
Viet Nam (Vietnamese)	Toi-mat	Mat	Kin	Pho Bien Han Che

* Provided that this level of protection is at least equivalent to that provided by the foreign government, but less than U.S. Confidential.

- (13) Radiographs and X rays. When standard markings are not practical on the radiograph or X ray, they must be placed on the jacket, folder, or similar covering. The user must ensure that the appropriately marked jacket, folder, or covering remains with the associated radiograph or X ray. If the radiograph or X ray contains standard markings, the jacket, folder, or covering must be marked according to 3.q.
- (14) Training Matter. Unclassified matter used to simulate or demonstrate classified matter for training purposes must be clearly marked to indicate it is unclassified. Examples of recommended training markings are as follows: "Training (Exhibit) Purposes Only," "Classified for Training Only," "Unclassified Sample," "Example (Exhibit) Only," or "Secret (Confidential) for Training Only." These markings should be in large print and should be placed so it is clear the marked information is *not* classified.
- (15) Aperture Cards. An aperture card is a punched, automatic data processing card on which a portion of a microfilmed document is mounted. Unclassified aperture cards are off-white and have the upper-left corner cut. Secret and Confidential images are on reddish stock without cut corners. The difference in color and the cut corner helps distinguish between the classified and unclassified aperture cards when they are commingled and stacked. Top Secret information should not be placed on an aperture card. The classification level should be marked near or above the microfilmed image on the face of the aperture card. The category (if RD or FRD) should be placed below the microfilmed image. If the classification level and category markings cannot be used, this information may be coded on the aperture card. The microfilm image should contain the classifier information, level, and category (if RD or FRD) in reduced size.
- (16) Classified Page Changes.
- (a) Periodic updates or revisions to a classified document may be transmitted as page changes instead of retransmitting the entire document. Individual page changes cannot be transmitted when the overall classification of the document has changed.
 - (b) The transmitting receipt for a page change should provide direction for incorporating the pages into the document.
 - 1 If the classified document is not accountable, the new pages may be inserted and the obsolete pages destroyed properly.
 - 2 If the classified document is accountable, the new pages may be inserted and the destruction of the obsolete pages documented according to local procedures. Although the

page changes themselves do not need to be given unique identification numbers, a record of the page changes must be kept.

- (c) Page changes must be marked in the same manner as the original document. For example, if the original document was portion marked, the page change must be portion marked, and if the category was marked on each page of the original document, it also must be marked on each page that is changed. Note: Also refer to 3.h.(2) which also contains requirements for marking page changes.
- q. File Folders and Other Containers. When not in approved secure storage containers, file folders and other items containing classified matter must be marked conspicuously to indicate the highest classification level of any classified matter contained within.
- (1) The classification level marking must be marked top and bottom on the front and back of the folder. The classification level marking is necessary only when the folder containing classified matter is removed from an approved secure storage repository (see Figure II-4).
 - (2) Containers of classified documents such as videotapes, cassettes, and ESM also must include classification level markings on the top and bottom of the front and back of the container. However, if the subject container is too small to contain typical classification labels on top and bottom, a single label may be placed in the middle of the case. When marked with the classification level, these containers act as cover sheets to alert observers about appropriate protection and handling requirements. If these containers are used for shipping, consider them an inner envelope only and address and mark them appropriately. (NOTE: The plastic encasing the actual tape, cassette, or ESM is not considered a container for the purposes of these marking instructions. Only the *removable* covering of a cassette, tape, or ESM is considered a container.)
- r. Transmittal Documents. The first page of a transmittal document must be marked with the highest level and category (if RD or FRD) of classified information being transmitted and with an appropriate notation to indicate its classification when the enclosures are removed. Additional markings (including category if RD or FRD) from the enclosure must be included on transmittal documents when they convey restrictions.
- (1) Unclassified Letters of Transmittal.
 - (a) If the letter of transmittal transmits a document containing RD or FRD or information with a caveat, the first page of the letter of transmittal must be marked on the lower left corner with the

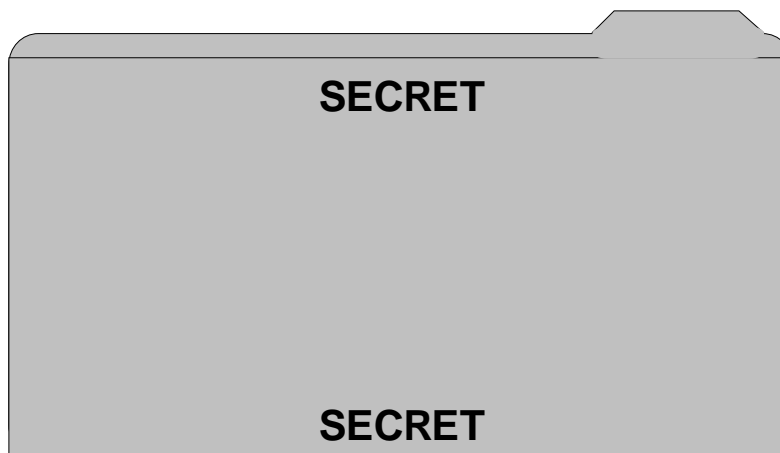
phrase, “Document transmitted herewith contains ____.” For example:

Document transmitted herewith contains: (insert classification level and category and/or caveat spelled out; e.g., Secret/Restricted Data).

- (b) Subsequent pages of an unclassified letter of transmittal require *no* classification markings.



Front



Back

Figure II-4. Example Markings for Classified File Folders

- (c) The following marking must be placed on the lower right corner of the letter of transmittal, with the classification level of the letter of transmittal (in this case, “Unclassified”) inserted.

When separated from enclosures, handle this document as:
(insert classification level and category and/or caveat spelled out; e.g., Secret/Restricted Data).

- (2) Classified Letters of Transmittal. Classified letters of transmittal must be handled in one of three ways.

- (a) The letter of transmittal and the attached document may be treated as a single document, with the letter of transmittal becoming part of the document. This method does not require the extra markings described below.
- (b) The letter of transmittal may be handled as a document separate from the transmitted document. This method does not require the extra markings described in paragraph (c) 2, below.
- (c) The final method, described below, allows for the letter of transmittal and the attached document to be transmitted together as one document but handled separately upon receipt.

- 1 The letter of transmittal must be marked with all required classification information. The first page of the letter of transmittal must be marked at the highest level contained in either the letter of transmittal or the transmitted document. If the letter of transmittal has multiple pages, each successive page must be marked at the top and bottom with the classification level of that page or the overall level and category (if RD or FRD) of the letter of transmittal.
- 2 The letter of transmittal must indicate the highest overall category (if RD or FRD) of information contained in the letter of transmittal and the transmitted document and any caveats. If the category of the information in the transmitted document is higher, this category information must be placed on the lower left corner of the letter of transmittal below the statement, “Document transmitted herewith contains,” as described above. If the letter of transmittal contains the higher category of information, this category information marking must be placed on the lower left corner of the letter of transmittal.
- 3 If the letter of transmittal is classified at a lower level than the information being transmitted, the classification level of

the letter of transmittal should be inserted after the phrase, “When separated from enclosures, handle this document as _____,” described above. When this type of letter of transmittal is received and separated from the transmitted document, the recipient needs no further authorization to change the classification markings on the letter of transmittal.

- s. Working Papers and Drafts. Classified working papers and drafts are considered to be interim production stages toward the generation of a permanent document.
- (1) Hard copies of working papers and drafts must contain the following markings:
 - (a) the date created;
 - (b) the highest potential overall classification level of the draft or working paper at the top and bottom of the outside of the cover page (if any), on the title page (if any), on the first page of text, and on the outside of the back cover or last page. Each interior page of a classified document must be marked at the top and bottom with the highest classification level of that page (including unclassified) or the overall classification of the document;
 - (c) the overall category (if RD or FRD) of the draft or working paper must be marked on the cover page (if any), title page (if any), or the first page of text. The category marking is not required on draft and working paper interior pages that contain RD or FRD information;
 - (d) the annotation “Working Paper” or “Draft” must be marked on the first page of text; and
 - (e) any applicable caveats or special markings must be annotated on the cover page (if any), title page (if any), or the first page of text.
 - (2) Electronic and facsimile versions of working papers and drafts are marked as required by paragraphs 3p(3) and (4).
 - (3) Classified working papers and drafts may be transmitted within work groups without being marked as final documents. Work groups may consist of individuals from multiple organizations (see 3.p.(3)(b)4.a.).
 - (4) Markings prescribed for a finished document must be applied when a draft or working paper meets the following requirements:
 - (a) released by the originator outside the activity or office;

- (b) retained for more than 180 days from the date of origin; or
 - (c) filed permanently.
 - (5) Classified documents that are updated on a frequent basis, commonly referred to as “living documents: (e.g. documents that are part of an ongoing experiment or study) may be considered as originating each date they are changed.
 - (a) Local procedures must provide a specific technique to demonstrate that the “living document” is in fact being changed frequently (e.g. a sheet attached to the front of the document that gives the number of pages and the date of the last change is an example of such a technique).
 - (b) Each version of a living document, that has been superseded by an updated version, retains its initially assigned origination date for the purposes of determining requirements for marking it as a finished document.
 - (6) See paragraph 1.e. for requirements for documents undergoing classification review.
- t. 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.
- u. Miscellaneous. Typewriter or printer ribbon cartridges and spools or carbons must be marked with the appropriate classification level and protected accordingly until destroyed. No additional markings are required.
- v. Other Government Agency (OGA) and Foreign Government Documents 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 remarked. However, all documents received must clearly indicate a classification level and category (if RD or FRD).
 - (1) OGA.
 - (a) If an accountable document arriving from another agency lacks a unique identification number, one must be assigned.
 - (b) When possible, returning documents because of improper marking should be avoided. Instead, the sender should be contacted and any marking issues resolved.

(2) Foreign Governments.

(a) Classified documents originated by a foreign government or international organization must either retain their original classification level markings or be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information. A classification officer should be contacted with any questions regarding the appropriate classification level for a foreign government document.

1 If the foreign marking is not readily understandable, the recipient must assign the equivalent U.S. marking (see Table II-2 for the foreign classification markings).

2 If there is no equivalent U.S. marking as required above, then the recipients or possessor must acquire the marking and protection requirements from the originating government.

3 Acceptable methods for assigning a U.S. classification level marking include, marking a document protector and placing the document inside, creating a transmittal document for the document, or placing a sticker with U.S. markings on the document. These practices will avoid marking up a document that may need to be returned to the foreign government.

4 Any markings provided must ensure a degree of protection equivalent to that required by the originating government or organization.

(b) Any markings provided must ensure a degree of protection equivalent to that required by the originating government or organization. A classification officer can answer any questions regarding the level of protection to assign a foreign government document.

w. Cover Sheets. Cover sheets must be applied to all classified documents when they are removed from a security container. The following SF cover sheets may be used: SF 703, Top Secret cover sheet; SF 704, Secret cover sheet; and SF 705, Confidential cover sheet (see www.archives.gov/isoo/security-forms/). Locally-developed cover sheets of the same color and format as the SFs may be used. Locally-created cover sheets may be overprinted with classification category (if RD or FRD), caveats (if applicable), and other information approved by the DOE cognizant security authority.

4. CONTROL SYSTEMS AND ACCOUNTABILITY.

- a. General. Control systems must be established and used to prevent unauthorized access to or removal of classified information. Accountability systems must provide a system of procedures that provide an audit trail. Accountability applies regardless of the physical form of the matter (e.g., electronic, paper, or parts).
- b. Accountable Matter. The following are types of accountable matter.
- (1) Top Secret matter.
 - (2) Secret matter stored outside an LA (or higher), including CREM marked as Secret.
 - (3) Any matter that requires accountability because of national, international, or programmatic requirements such as the following:
 - (a) classified computer equipment and media supporting the Nuclear Emergency Support Team (NEST) and Accident Response Group (ARG) operations and similar elements;
 - (b) national requirements such as cryptography and designated COMSEC;
 - (c) international requirements such as NATO ATOMAL, designated United Kingdom documents, or other FGI designated in international agreements; and
 - (d) special programmatic requirements (e.g., designated SAPs and Sigma 14).
 - (4) Classified Removable Electronic Media (CREM) which is required to be marked as S/RD or higher classification, or which is otherwise accountable [reference paragraphs 4.b.(2) and (3) above]. Each article of ACREM must remain in accountability until it is verifiable that none of the information that requires CREM to be accountable can be retrieved or recovered from that article. Only National Security Agency approved methods or other officially approved methods that comply with DOE cyber security policy may be used to determine whether information is recoverable from ACREM. Any such approved methods or criteria must be periodically performance tested to ensure that unauthorized access to classified information does not occur.
 - (5) Completed parts 2 and 2A of the SF 700, Security Container Information, for a container is an accountable document if any of the information stored

in that container is accountable. It does not, however, need to be placed into the formal accountability system; it must be accounted for according to local written procedures.

c. Accountable Classified Removable Electronic Media (ACREM) Custodians and Emergency Notification Personnel.

- (1) At least one appointed and trained ACREM custodian and one appointed and trained alternate ACREM custodian must be assigned for each vault, VTR, GSA-approved repository, or file cabinet used to store ACREM. If more than one custodian and one alternate custodian are assigned, the number of individuals assigned to these positions must be identified and justified through documented DOE CSA-approved procedures, and must be kept to the minimum number necessary based on operational need and associated risk, since additional custodians or alternates reduce the ability to fully account for all ACREM activities.
- (a) These appointed individuals are responsible and accountable for the ACREM, all associated accountability records, and other duties outlined in DOE cognizant security authority approved local procedures which must include, but are not limited to:
- (b) A formal and documented ACREM check out and transfer process must be implemented to record all ACREM transfers between ACREM custodians, alternate ACREM custodians, and users. This process must be performance tested to ensure its effectiveness, and must include:
- 1 Return of ACREM checked out from its normal storage location to its normal storage location at the close of the work shift. If operations needs, such as emergency deployments, dictate exceptions from this requirement, the exceptions must be fully documented and approved by the DOE cognizant security authority;
 - 2 Personal responsibility for the ACREM by the individual who checks it out (has it formally transferred to his/her control) until it is formally returned to its approved storage repository;
 - 3 Justifications in writing for deviations to Departmental ACREM requirements, due to National Security needs (e.g., uninterruptible testing). Deviation requirements are included in DOE M 470.4-1, *Program Planning and Management* and its CRD; and,

- 4 Training for all affected employees regarding ACREM procedures.
- (c) Strict limitation of access to all repositories storing ACREM to only the authorized ACREM custodians and their alternates.
- (2) Where an item of ACREM is in use across two or more work shifts, it is permissible to have one appointed custodian and one or more alternate custodian(s) per shift for the repository where the ACREM is stored. Where this arrangement is in effect, there must be a formal transfer and acknowledgement of the assumption of custodial responsibility by the arriving custodian. If the item of ACREM is in continuous use across the shifts, a formal transfer of accountability for the item must be recorded.
- (3) To preclude instances where ACREM is not available when needed due to the absence or incapacity of both the custodian(s) and alternate custodian(s), emergency notification personnel should be identified. These individuals must be listed on the SF 700, along with the listing of all other persons having the ability to obtain the combination to the repository. Part 1 of the SF 700 will be kept inside the repository and part 2 may be sent to:
- (a) another repository;
- (b) a central repository maintained for that purpose; or
- (c) a repository within a Central Alarm Station (CAS), provided that any individual with access to these repositories poses an access authorization at the level necessary for access to the material in the repository containing the ACREM.
- d. Control Stations. Control stations must be established and used to maintain records and access lists (when required) and control classified matter (including facsimiles) received by and/or dispatched from facilities. Employees must be designated and trained to operate these control stations and must have access authorizations commensurate with the level of their classified control responsibilities. A formally defined and operated ACREM accountability process may function as a control station.
- e. Accountability Records. Accountability records are required when accountable matter is originated, reproduced, transmitted, received, destroyed, or changed in classification. Control station operators must maintain accountability systems for accountable matter. All sites must develop procedures to ensure that all accountable matter has been entered into accountability systems. At a minimum, accountability records must indicate the following information for each accountable item.

- (1) Date of the Matter. The date the matter was originated or created. For documents, this term means the date the document was finalized.
- (2) Brief Description of the Matter (unclassified, if possible). Examples include the unclassified title (if a document) or description (if material). It may also be helpful to describe the form of the matter (e.g., a document, magnetic medium, microform, drawing, photograph, or photographic negative). If a title or description is classified, an unclassified descriptor should be used to prevent the accountability records system from becoming classified.
- (3) Unique Identification Number. This could be a unique document number (if a document) or serial number (if material). Unique identification numbers may be provided by creating a totally new number for each individual document, including copies, or by adding the copy and series to the old base number when reproducing accountable documents. The key point is to ensure that each document, whether an original or a reproduction, has some kind of unique number associated with it.
- (4) Classification Level (and Category, if RD or FRD) and Caveats. Classification level, category (if RD or FRD), and additional handling caveats, if any, of the matter must also be indicated.
- (5) Number of Copies and Disposition. The number of copies of a document (including the original) generated during either origination or reproduction, the disposition of each copy (e.g., destruction, downgrading, declassification, dispatch outside the facility, or incorporation into another accountability record), and the date of disposition. The term “disposition” varies in meaning as follows regarding:
 - (a) origination, transmission, receipt, and reproduction, “disposition” means the offices or activities where the matter was distributed;
 - (b) destruction, “disposition” means the organization where the matter was destroyed and by whom;
 - (c) change of classification, “disposition” means which office or activity performed the change of classification and which offices or activities have copies of the matter.
- (6) Originator Identification. The organization name and address of the originator. For material, this information is found in the associated paperwork.
- (7) Authority for Contractor Retention. Contract or other written retention authority that authorizes the matter to be in the possession of a contractor. This authorization can be either a letter of authorization or a contract

reference to the authorization to retain classified matter. A copy of this authorization should be maintained with the accountability records and should be readily available to facilitate compliance disposition reviews.

- (8) Date Received (if applicable). The date the transmitted matter arrived.
- (9) Activity from Which the Matter was Received (if applicable). The office or activity name and address from which matter was transmitted to the recipient.
- (10) The individual who checked it in and/or out (who has personal responsibility for it).

f. Inventory.

(1) Frequency.

- (a) All ACREM must be inventoried and all results documented on a recurrent basis. All discrepancies between ACREM records and the verified location and status of all ACREM must be identified and resolved (examples of status include possessed by an identified individual, stored, or destroyed).

1 The current and previous individual control/possession of all ACREM, according to their assigned custodians and users, must be documented and available at any given time within record retention periods that comply with the General Record Schedule 18, *Security and Protective Services Record*. Inventories and resolution of discrepancies must be used to validate that local ACREM custodians, alternate custodians, users and procedures are meeting this performance requirement; and

2 The baseline required frequency of the recurrent ACREM inventories is monthly (no longer than 31 calendar days between inventories). However, the DOE CSA may increase the time between inventories for specific repositories up to a maximum of six months. The DOE CSA's decision to decrease inventory frequency must be based on a documented determination that doing so will result in no unacceptable increased risk to the ACREM. Factors to consider in making this determination include the amount of ACREM, the number of formally appointed ACREM custodians and alternate custodians, ACREM usage levels, strength of the local Classified Matter Protection and Control Program, characteristics of the local facilities, equipment

and procedures, and past performance in managing ACREM; and

- 3 Inventories may be waived for ACREM that are maintained in a locked file cabinet or GSA-approved repository that is located in a vault or a VTR or are maintained in security containers with X-07, X-08, or X-09 (XO-Series) locks, and the container has not been accessed since the last inventory. However, time between inventories must not exceed one year (365 calendar days) for any ACREM.
- (b) NNSA's NEST, ARG, and similar elements' classified computer equipment and media must be inventoried at least once a month by two individuals. In addition, DOE cognizant security authorities must develop deployment and redeployment checklists for all ARG, NEST, and similar elements that include procedures for inventorying accountable equipment both before and after a deployment.
- (c) All other accountable matter must be inventoried no less frequently than every 12 months.
- (2) Inventories will 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.
- (3) Reports. Any unresolved discrepancies between the items found to be present and the inventory list must be reported and dealt with according to DOE policy and requirements for reporting incidents of security concern (see DOE M 470.4-1, *Safeguards and Security Program Planning and Management*).
- (4) Inventory Records. ACREM Custodians and/or Control station custodians must maintain records of the inventories and any reports generated as a result of the inventories (e.g., unaccounted for document reports).
- g. Records Disposition. Records maintained to control and account for classified matter, including those reflecting receipt, dispatch, and destruction, must be retained in accordance with the DOE records schedule and the NARA's GRS 18.
- h. 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 this GRS. These files must be scheduled on an SF 115, Request for Records Disposition Authority.

- i. Working Papers and Drafts. Classified working papers and drafts are considered to be interim production stages toward the generation of a permanent document. Working papers and drafts must be:
 - (1) protected in accordance with the assigned classification;
 - (2) destroyed when no longer needed; and
 - (3) accounted for and controlled in the manner prescribed for a finished document when the working papers and drafts meet the following requirements:
 - (a) released by the originator outside the originating activity or work group (a work group may consist of individuals from multiple organizations that is established to support the activity);
 - (b) retained for more than 180 days from the date of origin; or
 - (c) filed permanently.

- j. Automated Accountability Systems and Electronic Receipting.
 - (1) Automated Accountability Systems. Automated accountability systems must:
 - (a) be approved by the DOE cognizant security authority;
 - (b) implement the requirements under paragraph 4.e; and
 - (c) provide security controls to ensure that no unauthorized changes are made to system records.

 - (2) Electronic Receipting. The Information Security Oversight Office (ISOO) has approved the use of electronic receipting systems as long as the following conditions are met. The system:
 - (a) is approved by the DOE cognizant security authority;
 - (b) provides identification of both the individual and the document disposition; and
 - (c) provides adequate security controls to ensure that no unauthorized changes are made to the system record.

5. REPRODUCTION.

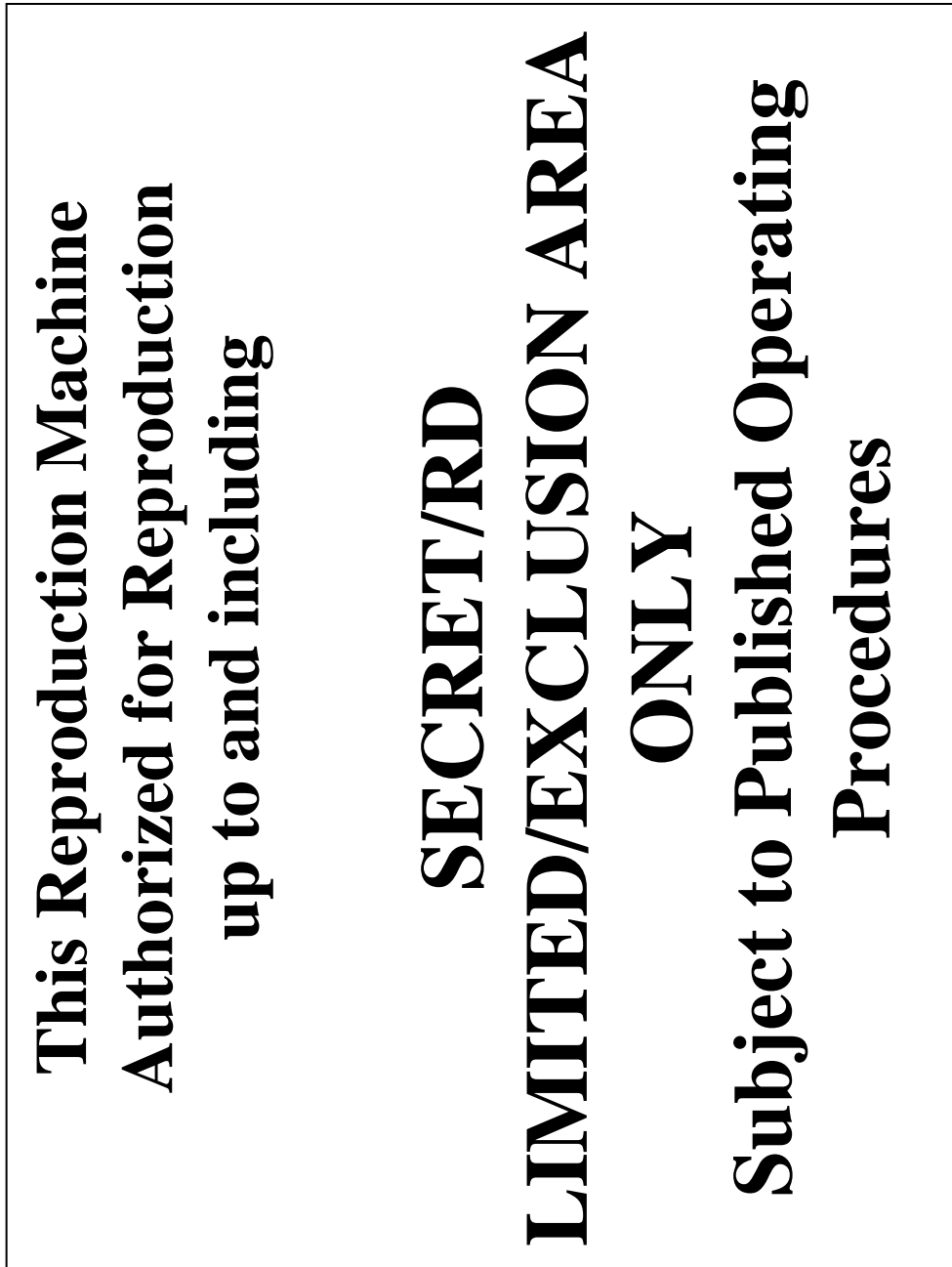
a. General.

- (1) Classified documents may be reproduced without originator approval except when they contain markings that limit reproduction without specific written originator approval.
- (2) ACREM may be reproduced when any of the data that resides on a piece of ACREM is to be copied onto a piece of media that has already been placed into the formal accountability system, provided there are no other limitations. Permission is required from the DOE cognizant security authority before copying any of the data that resides on a piece of ACREM onto a piece of media that has not already been placed into the formal accountability system.
- (3) If a classified document needs to be copied immediately, and the document contains a caveat limiting reproduction without originator approval, the following procedure must be used:
 - (a) gain originator approval by telephone;
 - (b) make the minimum number of copies required. Following normal procedures, destroy unneeded copies immediately after the emergency use; and
 - (c) follow up by obtaining permission in writing as soon as possible.
- (4) The cognizant security authority must establish local controls for the reproduction of classified documents. Reproduction of classified documents must be limited to the minimum number of copies consistent with operational requirements and any further reproduction limitations shown on the document. Local procedures should address the issue of controlling the number of copies of classified documents. To restrict reproduction of a classified document, consider one of the following techniques.
 - (a) For intelligence documents only, the Director of Central Intelligence ORCON caveat marking may be used to restrict reproduction to that allowed by the originator.
 - (b) Originators of non-intelligence documents who wish to prevent unlimited copying of a classified document may use the markings specified in paragraph 3.1.(7) or others similar in content.

- (5) Reproduction must be accomplished by authorized persons who know the procedures for classified reproduction and only in the performance of official or contractual duties.
 - (6) Reproduced copies are subject to the same protection and control requirements as the originals.
 - (7) Reproduction restrictions must not constrain the reproduction of documents to facilitate review for declassification. However, after such reviews, reproduced documents remaining classified must be destroyed in accordance with paragraph 8.
- b. Equipment. Classified documents must be reproduced on equipment specifically approved and designated for this purpose to ensure minimal risk of unauthorized disclosure. To the greatest extent possible, these machines must be located within LA, PAs, or EAs.
- (1) Access to Machines. Classified documents must be reproduced under appropriate security conditions to preclude unauthorized access to classified information. Classified copying must not be performed in the presence of individuals lacking the proper access authorizations.
 - (2) Notices. Notices regarding the restrictions and requirements of reproducing classified documents must be posted conspicuously next to the equipment (see Figures II-5 and II-6).
 - (3) Clearing. Ensure that no classified waste is trapped or left in the equipment and clear all possible residual classified images after classified reproduction. Local procedures and copier design will dictate how the copier should be sanitized.
 - (4) Approval. Ensure that all machines to be used for reproducing classified documents are approved in accordance with local procedures and cyber security policy. At a minimum, ensure that:
 - (a) classified copy machines do *not* have modems or the ability to be connected to an external modem; and
 - (b) contracts for new digital copy machines specify that memory chips will *not* be removed without permission and that any remote diagnostics capabilities will be disabled.
 - (c) In areas where routine Technical Surveillance Countermeasures (TSCM) services occur, reproduction machines must be examined by a certified TSCM team prior to introduction into the area.

c. Documents Sent To or Received From Outside Agencies.

- (1) Documents Sent to Outside Agencies. To ensure that a document sent to an outside agency is not reproduced without the originator's consent, a caveat limiting such further reproduction must be placed on the document. Documents without such markings may be reproduced by the other agency.



**Figure II-5. Notice Regarding Restrictions on Reproducing
Classified Information**

- (2) Documents Received from Outside Agencies. Outside agency documents may be reproduced in accordance with the same rules and restrictions that exist for DOE documents. Therefore, unless specific instructions to the contrary accompany the documents, they may be reproduced. For example, National Security Council (NSC) documents will have a copy restriction notice; therefore, NSC documents will be reproduced only with the permission of the originator.

**CLASSIFIED REPRODUCTION PROCEDURAL INSTRUCTIONS
(Within Limited/Exclusion Area)**

1. See the "Authorization Poster" for classification limits and restrictions.
2. Limit observation of classified operations to persons with appropriate clearance and need-to-know.
3. Require reproduction authorization for ORCON or other control caveats that limit or prohibit reproduction without specific permission.
4. Limit number of copies to only those that are absolutely required. If the subject document is in accountability, all copies must also be brought into accountability.
5. Destroy unacceptable or excess copies following DOE and local destruction procedures for classified waste (accountability and destruction receipts not required).
6. Run (insert required number) blank copies through the machine after copying operations are completed, and check the last copy for images. If images are still present, continue running copies until no images remain. Destroy the blank copies as classified waste. Accountability and destruction records are not required.
7. Double-check the copying area before departing to ensure no classified matter remains (i.e., originals removed from copying plate, copies removed from machine collection tray or collating bins, and copies to be destroyed collected).

Figure II-6. Classified Reproduction Procedural Instructions

6. RECEIVING AND TRANSMITTING CLASSIFIED MATTER.
- a. General. Classified matter must be transmitted only in the performance of official or contractual duties. If the transmission is not required by the specific terms of

the contract or required for performance of the contract, contractors must obtain written authorization from the DOE cognizant security authority before transmitting classified matter outside the facility. Before transmitting classified matter, the sender must ensure that the recipient has the appropriate access authorization or clearance, has any required programmatic or special access approval, meets the need-to-know criteria, and has an approved classified address.

- b. Receiving. When classified matter is received at a facility, the following controls must apply (also see paragraph 6.d.):
- (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. Though the inner envelope must not be opened before delivery at the control station, the outer envelope may be opened if local procedures permit.
 - (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 cognizant security authority. 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 shipment is in order and includes a receipt, the receipt must be signed and returned to the sender. A copy of the receipt must be maintained with the control station records.
- 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.
- (1) Envelopes and Similar Wrappers.
 - (a) When envelopes are used for packaging, the classified information must be protected from direct contact with the inner envelope. This is accomplished by having a cover sheet on the front of the document and a sheet of paper or cover sheet to protect the back of the document if the document has information on the back page.
 - 1 The overall classification level of the contents must be marked on the top and bottom of the front and back of the inner container.
 - 2 The category (if RD or FRD) and caveats (if applicable) or special markings must be placed on the front of the inner container.

- 3 The inner container must be sealed. The sender's classified address should appear in the upper left corner and the recipient's classified address should be centered on the front of the container.
 - 4 The outer envelope or container must be sealed and marked with the recipient's and sender's classified mailing addresses (mailing, shipping, or overnight, as appropriate).
 - 5 The outer envelope must not carry markings indicating the contents are classified.
- (b) When opaque containers (i.e., envelopes) are temporarily unavailable, appropriate measures must be taken to ensure that the contents of the document cannot be seen through the inner container and that the security markings on the inner container cannot be seen through the outer container.
- (c) All the seams of an envelope or wrapper must be sealed with tamper-resistant tape (e.g., fiber tape) or be constructed in a manner designed to provide tamper indication (e.g., tamper-evidence security bags) to prevent undetected access to the contents while in transit.

NOTE: Outer containers must meet U.S. Postal Service regulations for registered packages.

- (2) Other Containers. If the item is of a size, bulk, weight, or nature that precludes the use of envelopes for packaging, other containers of sufficient strength and durability must be used to protect the item while in transit.
- (a) To prevent items from breaking out and to facilitate the detection of tampering, tamper-resistant material (such as seals, puncture resistant material, or wire mesh) must be used for packaging.
 - (b) As long as the item is enclosed in a double container, the matter may be wrapped or boxed in paper, wood, metal, or a combination thereof.
 - (c) The inner package must be addressed to a classified address, return-addressed to a classified address, and marked with the overall classification level and category (if RD or FRD) of the contents and any appropriate caveats.
 - (d) 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.

- (e) If specialized shipping containers, including closed cargo transporters, are used for transmitting classified matter, the shipping container may be considered the outer container.
 - 1 The address may be omitted from the inner and outer container for shipments in full truckload lots when such an exception is contained in the provisions of the contract.
 - 2 Under no circumstances will the outer container or the shipping document attached to the outer container reflect the classification of the contents or the fact that the contents are classified.

(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. The shell or body must be marked with the classification level and category (if RD or FRD) of the equipment, but the address and return address may be omitted. The outer container must be addressed to a classified address, return-addressed to a classified mailing address, and sealed with no markings or notations to indicate the contents are classified.
- (b) If the classified matter is an inaccessible internal component of a bulky item of equipment, such as a missile, that 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. If the shell or body is classified, the matter must be draped with an opaque covering that will conceal all classified features. The covering must be capable of being secured to prevent inadvertent exposure of the item.

(4) Locked Briefcases. If a locked briefcase is used to hand-carry classified matter of any level, the briefcase may serve as the outer container. The requirement that an individual carrying a briefcase with classified matter outside a security area must possess a DOE Form (F) 5635.13, Authority to Hand-Carry Classified Matter, is no longer in effect. If local procedures require use of hand-carry cards, sites may develop local hand-carry forms.

- (a) The inner container must be sealed, addressed with the sender's and recipient's classified addresses, and marked with the overall classification level and category (if RD or FRD) of the contents and caveats (if applicable).

- (b) The briefcase (outer container) must indicate the return classified address and must contain no markings to indicate the contents are classified.
 - (c) A briefcase may not serve as the outer container for travel aboard commercial aircraft.
- d. Offsite Transmittal and Receipts. DOE F 5635.3, Classified Document Receipt, or a receipt comparable in content must be used to transmit accountable and classified matter outside of facilities. Receipts must identify the classified contents and the names and addresses of both the sending and receiving facilities. Receipts must not contain classified information. The receipt must be placed inside the inner container. 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, or a receipt comparable in content must be used (see Figures II-7a and b).
 - (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) classified address of the sender;
 - (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 Items. If all items are going to one recipient, one receipt may be used for multiple items. Regardless of the number of items being transmitted, one receipt should be completed for each recipient. Check any special mailing instructions included in the classified mailing address in the Safeguards and Security Information Management System (SSIMS).

DOE F 5635.3 (09-95) 05-94 editions may be used		U.S. DEPARTMENT OF ENERGY CLASSIFIED DOCUMENT RECEIPT			OMB Control No. 1910-1800 OMB Burden Disclosure Statement on Reverse	
TO				POSTAL NUMBER		
				DATE MAILED		
				INSTRUCTIONS 1. Verify addressee's classified mailing address. 2. Describe document by subject or title and originator. See DOE 5635.1A for when this form is required. 3. Show classification and extra markings. 4. Forward original and duplicate to addressee. 5. Retain copy pending return of signed original by addressee.		
FROM						
DESCRIPTION OF DOCUMENT (Subject or title and originator)	IDENTIFICATION NUMBER	DATE OF DOCUMENT	COPY and SERIES	NUMBER of PAGES		
<i>I have received the document(s) listed above and assume responsibility for safeguarding in accordance with security regulations.</i>						
Signature of addressee or name of addressee and signature of recipient: _____ Date: _____						
Received for addressee by: _____ Date: _____ <small>(to be used only by mail rooms)</small>						
1. Return to Sender		2. Addressee's Copy		3. Pending		

Figure II-7a. DOE F 5635.3, Classified Document Receipt

OMB BURDEN DISCLOSURE STATEMENT

Public reporting burden for this collection of information is estimated to average 10 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Office of Information Management Program Management Group, Records Management Team, HR-424-GTN, Paperwork Reduction Project (1910-1800), U.S. Department of Energy, 1000 Independence Avenue, S.W., Washington, D.C. 20585; and to the Office of Management and Budget (OMB), Paperwork Reduction Project (1910-1800), Washington, D.C. 20503.

Figure II-7b. DOE F 5635.3, Classified Document Receipt, OMB Burden Disclosure Statement

- (3) Exceptions. Receipts are not required for non-accountable classified matter under the following conditions:
 - (a) transmittal of matter within a facility; or
 - (b) transmittal of Confidential matter.
- (4) Facsimile Transmission. Individuals transmitting classified information through facsimile systems must confirm receipt (verbally or in writing) with the intended recipient.
 - (a) A receipt, such as DOE F 5635.3, may be completed and transmitted with the classified message by means of facsimile systems. Upon receiving the facsimile, the recipient would complete the receipt and return it also by facsimile.
 - (b) An acceptable alternative would be to contact the intended recipient and notify him/her that a classified message is being transmitted by facsimile. Upon receipt, the recipient must telephone the sender to verify the complete transmission was received. This verbal communication must be documented and retained and will suffice for all other written forms of receipt.
- (5) 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. Although non-accountable Confidential matter transmitted outside a facility *does not* require a receipt, if a receipt is submitted it must be signed and returned to the sender.

- (6) Suspense Copies. When a receipt is used, a duplicate copy of the receipt must be maintained in a “suspense” file at the control station until the signed receipt is returned.
 - (a) Procedures should be established for both tracking the return of receipts and the actions required if receipts are not returned.
 - (b) A suspense date (normally not to exceed 30 days) must be established, and follow-up action must be initiated if the signed receipt is not returned within the suspense period.
 - (c) If the follow-up action is unsuccessful, an inquiry must be conducted and the possible loss of the matter must be reported in accordance with incident reporting requirements.
 - (d) Copies of signed receipts for classified matter must be retained at control stations in accordance with the DOE records schedule and the NARA GRSs.
- (7) Electronic Receipting. The ISOO has approved the use of electronic receipting under the following conditions.
 - (a) The system must provide a method to ensure electronic signature integrity.
 - (b) The system must be able to provide verification of individuals and show either the individual possessing the document or the disposition made of the document.
 - (c) The system is approved by the DOE cognizant security authority.

e. Classified Addresses.

- (1) Classified matter must be addressed only to approved classified addresses for mailing, shipping, or overnight delivery, contingent upon the appropriate method of transmission.
- (2) Classified addresses must be verified through SSIMS, except as otherwise noted in this Manual, for:
 - (a) companies where there is a DOE contractual interest;
 - (b) OGA contractors where there is no contractual agreement with DOE, and the interest includes RD, FRD, or weapons data information; and

(c) companies where there is no DOE contractual agreement for NSI.
Note: Defense Security Service (DSS) may also be used for verifying classified addresses approved for NSI.

- (3) Hardcopies of classified addresses obtained through SSIMS or DSS are only valid for 30 calendar days.
- (4) A Classified Mail Channel may be established in SSIMS for an OGA contractor organization where DOE or NNSA does not have a contractual interest. To establish an address for the Classified Mail Channel, a Statement of Security Assurance, or a form comparable in content, must be completed and signed by the cognizant security authority and authorizing Government official for the OGA contractor (see Figures II-8a and II-8b for a copy of and instructions for a Statement of Security Assurance). Also see DOE M 470.4-1, *Safeguards and Security Program Planning and Management, Facility Clearance Program*.

Once the form is completed, the information must be entered into SSIMS. This process may only be used when the contractor facility has been approved by another Government agency and registered in SSIMS and must not be used as a basis for granting facility security approvals.

- (5) Alternative methods for verifying classified addresses must be approved by the Office of Health, Safety and Security.
- (6) Office code letters, numbers, or phrases must be used in an attention line for internal routing. A recipient's name may be used in addition to office code letters, numbers, or phrases.
- (7) When classified matter must be sent to an individual or consultant operating at a cleared facility other than his or her own, or when classified matter must be sent to any approved facility at which only one cleared employee is assigned, the outer container must specify the following:

TO BE OPENED BY ADDRESSEE ONLY.

Postmaster—Do Not Forward. If Undeliverable to Addressee, Return to Sender.

- (8) Mail addressed as indicated in paragraph 6.e.(7) above must be accepted only by the addressee or by an agent the addressee has authorized in writing to receive such mail. Only personnel who have an appropriate access authorization may be designated as agents for the addressee.

STATEMENT OF SECURITY ASSURANCE																																			
In fulfillment of the requirements set forth by the U.S. Department of Energy (DOE), this statement of security assurance is being submitted on the following facility.																																			
1. ACTION: <input type="checkbox"/> Visit Request <input type="checkbox"/> Classified Mail Channel <input type="checkbox"/> New <input type="checkbox"/> Update	2. HOST ENTITY NAME AND ADDRESS:	3. HOST ENTITY Facility Code: Cage Code: Level & Category: MOU Date:																																	
4. OGA CONTRACTOR FACILITY NAME AND PHYSICAL LOCATION:																																			
5. UNCLASSIFIED MAILING ADDRESS:		6. CLASSIFIED MAILING ADDRESS: (Contractors must include cage code, facility clearance, and date granted)																																	
7. CLASSIFIED SHIPPING ADDRESS:		8. CLASSIFIED OVERNIGHT ADDRESS:																																	
1. ACCESS LEVELS: The above CLASSIFIED addresses are approved for this contractor facility to receive and store classified information at all of the following levels, categories, and special markings that are checked:																																			
<table style="width: 100%; border: none;"> <tr> <td style="width: 25%;">Facility Clearance:</td> <td style="width: 25%;">Top Secret Level <input type="checkbox"/></td> <td style="width: 25%;">Restricted Data Category</td> <td style="width: 25%;"></td> </tr> <tr> <td><input type="checkbox"/></td> <td>CNWDI <input type="checkbox"/></td> <td>Secret Level <input type="checkbox"/></td> <td>Formerly Restricted Data</td> </tr> <tr> <td>Category <input type="checkbox"/></td> <td>Weapons Data <input type="checkbox"/></td> <td>Confidential Level <input type="checkbox"/></td> <td>National Security Information Category</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Sigmas</td> <td></td> <td></td> </tr> <tr> <td>Storage Capability:</td> <td>Top Secret Level <input type="checkbox"/></td> <td>Restricted Data Category</td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td>CNWDI <input type="checkbox"/></td> <td>Secret Level <input type="checkbox"/></td> <td>Formerly Restricted Data</td> </tr> <tr> <td>Category <input type="checkbox"/></td> <td>Weapons Data <input type="checkbox"/></td> <td>Confidential Level <input type="checkbox"/></td> <td>National Security Information Category</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Sigmas</td> <td></td> <td></td> </tr> </table>				Facility Clearance:	Top Secret Level <input type="checkbox"/>	Restricted Data Category		<input type="checkbox"/>	CNWDI <input type="checkbox"/>	Secret Level <input type="checkbox"/>	Formerly Restricted Data	Category <input type="checkbox"/>	Weapons Data <input type="checkbox"/>	Confidential Level <input type="checkbox"/>	National Security Information Category	<input type="checkbox"/>	Sigmas			Storage Capability:	Top Secret Level <input type="checkbox"/>	Restricted Data Category		<input type="checkbox"/>	CNWDI <input type="checkbox"/>	Secret Level <input type="checkbox"/>	Formerly Restricted Data	Category <input type="checkbox"/>	Weapons Data <input type="checkbox"/>	Confidential Level <input type="checkbox"/>	National Security Information Category	<input type="checkbox"/>	Sigmas		
Facility Clearance:	Top Secret Level <input type="checkbox"/>	Restricted Data Category																																	
<input type="checkbox"/>	CNWDI <input type="checkbox"/>	Secret Level <input type="checkbox"/>	Formerly Restricted Data																																
Category <input type="checkbox"/>	Weapons Data <input type="checkbox"/>	Confidential Level <input type="checkbox"/>	National Security Information Category																																
<input type="checkbox"/>	Sigmas																																		
Storage Capability:	Top Secret Level <input type="checkbox"/>	Restricted Data Category																																	
<input type="checkbox"/>	CNWDI <input type="checkbox"/>	Secret Level <input type="checkbox"/>	Formerly Restricted Data																																
Category <input type="checkbox"/>	Weapons Data <input type="checkbox"/>	Confidential Level <input type="checkbox"/>	National Security Information Category																																
<input type="checkbox"/>	Sigmas																																		
Material Classification Level: _____																																			
2. CERTIFICATIONS																																			
DOE classified matter in the possession of this office will be stored and protected in accordance with Executive Order 12958 as amended, and its implementing directives *including the Atomic Energy Act of 1954, as amended.). Access to Restricted Data and Formerly Restricted Data will only be granted to those individuals who have a need-to-know and have proper access in accordance with the Atomic Energy Act of 1954, as amended. Such classified matter in the possession of this office will not be turned over to any contractor or subcontractor engaged by this office unless approved by DOE.																																			
IF AT ANY TIME THE ADDRESS (UNCLASSIFIED OR CLASSIFIED) LISTED ABOVE CHANGES, PLEASE NOTIFY THE DOE OFFICE BY PROVIDING AN UPDATED STATEMENT OF SECURITY ASSURANCE.																																			
ALL PARTS OF THIS STATEMENT MUST BE COMPLETED AND AGREED TO BY THE COGNIZANT SECURITY OFFICER. THE UNDERSIGNED ATTESTS TO ALL OF THE ABOVE STATEMENTS.																																			
_____ Typed Name and Organization of Cognizant Security Officer		_____ Cognizant Security Officer Signature																																	
_____ Typed Name and Title, Authorizing Government Official		_____ Authorizing Government Official Signature																																	
_____ Date		_____ Phone																																	
_____ Date		_____ Phone																																	

Figure II-8a. Statement of Security Assurance

**INSTRUCTIONS FOR COMPLETING THE STATEMENT OF SECURITY ASSURANCE
TO ESTABLISH CLASSIFIED MAIL CHANNELS FOR NON-DOE
OR NON-NNSA CONTRACTORS**

- Item 1: ACTION:** Select the appropriate box showing the reason for completing the form.
- Item 2: HOST ENTITY NAME AND ADDRESS:** Provide the name and address of the user agency.
- Item 3: HOST ENTITY:**
- FACILITY CODE:** Provide the facility code assigned by DOE.
 - CAGE CODE:** Enter the DOE cage code.
 - LEVEL AND CATEGORY:** Enter the level and category of the facility.
 - MOU DATE:** Provide the date of the MOU between DOD or other Government agency (OGA) and DOE.
- Item 4: OGA CONTRACTOR FACILITY NAME AND PHYSICAL LOCATION:** Show the contractor name and the address that designates the facility's actual location. Give the precise street address or location to identify the facility; do not use a Post Office box number as a location.
- Item 5: UNCLASSIFIED MAILING ADDRESS:** Provide the facility's unclassified mailing address for routine correspondence.
- Item 6: CLASSIFIED MAILING ADDRESS:** Provide the facility's current classified mailing address, approved to receive classified matter through the U.S. Postal Service. Contractors must include cage code and facility clearance and date granted.
- Item 7: CLASSIFIED SHIPPING ADDRESS:** Provide the full U.S. Postal Service address for shipping classified material (e.g., equipment, parts, and assemblies, including nuclear material). For commercial carriers, enter DNA (does not apply) unless the carrier itself maintains an address at which to receive classified material.
- Item 8: CLASSIFIED OVERNIGHT ADDRESS:** Enter the name of the approved overnight classified mail delivery address or identify the common carrier service. Enter the address to be used for shipping classified matter when using a commercial carrier.
- Item 9: ACCESS LEVELS:**
- Facility Clearance:** Identify the highest classification level and mark each category of approval for classified information that can be accessed by the facility's employees.
 - Storage Capability:** Identify the highest classification level and category of classified matter approved to be stored at the facility.
 - Material Classification Level:** Enter the highest classification level of material (e.g., equipment, parts, assemblies).
- Item 10: CERTIFICATIONS:** Provide the signature; title; and telephone number, with area code, of the facility cognizant security officer and the authorizing Government official.

Figure II-8b. Statement of Security Assurances, Instructions

- f. Transmittal and Receipt within Facilities. Classified matter transmitted within a facility must be prepared to ensure adequate security protection is applied at the appropriate classification level and category for the classified matter involved and the method of transmission. Double-wrapping is not required (except as noted); however, in all cases, measures must be taken to protect against unauthorized disclosure.
- (1) The matter may be transmitted by the following:
 - (a) Personnel who have appropriate access authorization for the classification level and category of classified information involved.
 - (b) Approved electronic means. When using this method, both the transmitting and receiving systems must be approved for the classification level and category of the information to be transmitted. Facilities also must have an approved security plan and procedures for transmitting the information by electronic means.
 - (2) Although double-wrapping is not required for classified matter transmitted within a facility, the transmittal method should dictate the most suitable method of protection.
 - (a) If the classified matter is hand-delivered by the sender to the intended recipient, the matter must be covered by some form of protective covering to preclude unauthorized view.
 - (b) If the classified matter is transmitted by site delivery personnel, it must be placed within a container to prevent exposure during transfer.
- g. Transmitting Top Secret Matter Outside of Facilities.
- (1) Top Secret matter may be transmitted by the Defense Courier Service or the Department of State Courier System.
 - (2) Top Secret matter may be transmitted over approved communications networks. See DOE O 200.1, *Information Management Program*, dated 9-30-96, for secure communications requirements.
 - (3) Individuals may be authorized to hand-carry Top Secret matter in accordance with paragraph 6.j.
- h. Transmitting Secret Matter Outside of Facilities.
- (1) Secret matter may be transmitted by any method approved for the transmission of Top Secret matter.

- (2) Secret matter also may be transmitted through the following postal/mail services.
 - (a) Secret matter may be transmitted through the U.S. Postal Service Registered Mail within the 50 States, the District of Columbia, and Puerto Rico. Transmission of COMSEC material or COMSEC keying material via the U.S. Postal Service is not permitted (see DOE M 200.1-1, *Telecommunications Security Manual*, for approved methods of transmission). A return receipt is not required for U.S. Postal Service Registered Mail.
 - (b) Secret matter may be transmitted by U.S. Registered Mail through Army, Navy, or Air Force Postal Service facilities, provided approval is obtained from the 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) Secret matter may be transmitted to and between United States Government and Canadian Government installations in the 50 States, the District of Columbia, and Canada using Canadian registered mail with registered mail receipt.
 - (d) DOE and DOE 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 DOE and DOE contractors.
 - (e) Secret matter may be transmitted by approved commercial express service organizations in accordance with the provisions contained in paragraph 6.k.
 - (f) Secret matter may be transmitted by approved common carrier services with escorts who possess the appropriate access authorization in accordance with paragraph 6.l. upon approval by the cognizant security authority.
- i. Transmitting Confidential Matter Outside of Facilities.
 - (1) Confidential matter may be transmitted by any method approved for the transmission of Secret matter.
 - (2) Confidential matter may be transmitted by U.S. Postal Service Certified Mail within the 50 States, the District of Columbia, Puerto Rico, and U.S. territories or possessions. Use of the U.S. Postal Service is not permitted

for the transmission of COMSEC material or COMSEC keying material (see DOE M 200.1-1, *Telecommunications Security Manual*, for approval methods of transmission). 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 DOE.

- (3) DOE and DOE 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 DOE and DOE contractors.

j. Hand Carrying. The following requirements apply to hand-carrying classified matter; however, the requirements identified in paragraph 6.l. also apply to hand-carrying bulk documents.

- (1) Local procedures must be developed to explain the process for obtaining approval to hand-carry outside of a facility and for providing notification when removing classified matter from the facility.
 - (a) Line management must designate in writing the individuals authorized to approve employees to hand-carry or escort classified matter.
 - (b) Line management must be able to identify the individuals authorized to hand-carry.
- (2) The cognizant security authority identified on DOE F 470.2, Facility Data and Approval Record, or his/her designee must be notified whenever classified matter is to be hand-carried outside of the facility to ensure that appropriate protection measures are implemented. A record of the classified matter must be made before departure. A copy of the record must be carried by the employee. When he/she returns to the facility, an inventory must be made of the matter for which the employee was charged. The designated person/organization will approve employees to hand-carry or escort classified matter outside a facility only after a determination has been made that the following has occurred:
 - (a) an unusual situation warrants such action;
 - (b) the classified matter is not available at the destination;
 - (c) the time constraints do not permit transmission by other authorized methods;
 - (d) the classified matter can be properly handled and protected during transmission;

- (e) the transmission can be completed successfully on the same day;
 - (f) the classified matter can be stored appropriately upon arrival; and
 - (g) contingency plans for delayed arrival (i.e., unscheduled overnight delay outside the destination area) have been developed and approved by the cognizant security authority.
- (3) Only the classified matter absolutely essential for the purpose of the visit or meeting may be hand-carried by the employee. Individuals who hand-carry classified matter must have access authorizations commensurate with the level of the information involved and be aware of their responsibility to protect classified information.
- (4) The removal of classified matter from approved facilities to private residences or other unapproved places (e.g., hotel or motel rooms) is prohibited. Therefore, travelers anticipating a destination arrival time outside normal duty hours must make prior arrangements for storage of classified matter through the host security office.
- (a) All classified matter, when not in the possession of authorized individuals, must be stored only in DOE-approved facilities or as specified in approved contingency plans.
 - (b) Arrangements must be made in advance of departure for overnight storage at an approved facility that has appropriate storage capability.
- (5) Contingency plans for delayed arrival must cover alternative protection and storage procedures and reporting requirements and be approved by the cognizant security authority. Sites are not required to develop specific contingency plans each time a person hand-carries classified matter.
- (6) Classified matter may be hand-carried outside the United States, provided the following conditions are met.
- (a) The traveler must possess appropriate access authorization 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 Department of State.)
 - (b) The traveler must obtain written authorization from the Office of Health, Safety and Security. The authorization to hand-carry classified matter outside the United States is strongly discouraged and must be limited to situations with a strong justification for authorization. In all cases, authority for hand-carrying classified

matter outside the United States must be provided by the Office of Health, Safety and Security.

- (c) Individuals authorized to hand-carry classified matter outside the United States must possess a Nonprofessional Courier Letter signed by the Director, Office of Health, Safety and Security.
- (7) Classified matter may be hand-carried aboard commercial passenger aircraft by cleared employees with the approval of the cognizant security authority. The DOE cognizant security authority must establish criteria that must be met for acquiring each approval, and must also be able to confirm the approval for each instance of hand-carry prior to the traveler's arrival at the airport. Further requirements for security screening of classified matter at airports are established by the Transportation Security Administration (TSA). Information regarding these requirements may be requested from the DOE Office of Health, Safety and Security.
- (8) A record of all hand-carried accountable classified matter must be maintained both at the facility and with the individual transporting the matter. Receipts must be prepared in accordance with paragraph 6.d. of this Chapter. The record should contain the following information:
 - (a) subject or title (unclassified, if possible);
 - (b) date of the matter;
 - (c) date the matter was removed from the facility;
 - (d) signature of the person removing the matter; and
 - (e) date the matter was returned.
- k. Commercial Express Service Organizations. The use of commercial express delivery service for transmitting classified matter is restricted to emergency situations when the information positively has to be at the receiving facilities on the next working day. Commercial express service must not be used as a matter of routine or convenience for transmitting classified matter.
 - (1) General. At a minimum, the sender must ensure that the following conditions are met.
 - (a) The express service organization has been approved by the cognizant security authority and the Office of Health, Safety and Security.

- (b) The transmittal address, identified in SSIMS as the Overnight/Classified Common Carrier Address, is used on all wrappers.
- (c) The intended recipients are notified of the proposed shipments and arrival dates.
- (d) All packages are double wrapped before being inserted into the packaging provided by the commercial express service organization.
- (e) 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.
- (f) Because express terminals, as a matter of policy, are not approved for storage of classified matter, overnight service is not used on Fridays or on the day preceding a holiday unless prior assurance has been received from the intended recipients that someone will be available to receive the shipments on arrival at the facilities.

(2) Federal Express and Similar Commercial Express Service Providers. Federal Express is approved to provide shipments of classified matter and overnight carrier service. Other commercial carriers (e.g., Ross Air) may be used if they are approved by the cognizant security authority and are listed in SSIMS. In addition to meeting the requirements listed in 6.k.(1), the following requirements apply.

- (a) In accordance with packaging requirements, Federal Express packages must not be identified as classified shipments either by telling Federal Express employees or by marking the outer packages as classified.
- (b) All standard address requirements must be met. Shipments must be addressed only to overnight/classified common carrier addresses identified in SSIMS. The address selected for the overnight/classified common carrier address cannot be greater than five lines, *cannot* be a post office box, and must be a street address. Do *not* use terms such as “Document Custodian” in the address; however, the custodian’s name may be used.
- (c) Cognizant security authority adding overnight/classified common carrier addresses to SSIMS must (according to SSIMS requirements) indicate whether the address is for shipment by Federal Express or other commercial carrier.

- (d) Before establishing an address in SSIMS, cognizant security authorities should review internal local procedures to ensure that packages are opened only by appropriately cleared personnel.
 - (e) Federal Express business locations must not be granted DOE facility clearances, and Federal Express employees must not be processed for access authorizations. Facilities should include specific details regarding the use of Federal Express in local procedures.
 - (f) Federal Express drop boxes must not be used for classified shipments.
 - (g) Federal Express offers overnight freight service for packages weighing 150 to 750 lbs. Packages weighing more than 750 lbs. require prior notice. Federal Express may be contacted for details.
- (3) Problems. Problems with the delivery of classified matter via Federal Express or other commercial express service delivery must be reported in accordance with reporting of security incidents (see DOE M 470.4-1, *Safeguards and Security Planning and Program Management*). Packages not delivered in the specified timeframe are to be reported initially as an Impact Measurement Index (IMI)-1.
1. 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, as well as bulk shipments of classified matter.
- (1) General.
 - (a) Contents must be securely packaged and must meet applicable regulations (including those of the Department of Transportation).
 - (b) Seals or other tamper-resistant devices must be placed in a manner to show evidence of tampering. The type of seal to be used should be determined by the cognizant security authority. 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 during the same working day unless the carrier provides continuous protective service to the address of the consignee under locally approved procedures.

(2) Assurances and Notifications.

- (a) The carrier must have a facility clearance and a favorable Foreign Ownership, Control, or Influence determination (see DOE M 470.4-1, *Safeguards and Security Program Planning and Management*).
- (b) Notification of shipments must be transmitted to the consignee before departure with sufficient time 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.
- (c) 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 access authorization 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 appropriate access authorization 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, personnel escorting the shipments must travel in an escort car accompanying the shipments, keeping the shipment cars under observation. When practical, and time permits, personnel escorting shipments must check the cars, container locks, and/or tamper-indicating devices. Escort personnel should act as liaisons with train crews, other railroad personnel, special police, and law enforcement agencies, as appropriate.
- (d) When shipments are transported by motor vehicles, personnel escorting the shipments must maintain continuous vigilance for the presence of conditions or situations that might threaten the security of the cargo and take appropriate action, as circumstances require, to avoid interference with the continuous safe passage of the vehicles. During stops or layovers, personnel escorting shipments must check the tamper-indicating devices and locks.
- (e) The identity and authorization of persons who pick up classified matter must be verified.

7. CONTRACT CLOSEOUT/FACILITY CLEARANCE TERMINATION.

- a. General. Classified matter received or generated in the performance of a classified contract must be returned to DOE on completion of the contract unless the matter has been declassified or destroyed or retention is authorized. DOE M 470.4-1, *Safeguards and Security Program Planning and Management*, and this Section require that line management must implement the procedures developed by the cognizant DOE line management in coordination with the DOE cognizant security authority for contract closeout and facility termination.
- b. Contract Completion. When a contract is completed, the contractor usually destroys or returns all classified matter unless it provides a benefit to DOE for the contractor to retain the classified matter. Upon completion or termination of a contract, the contractor must submit to the contracting officer either a certificate of non-possession or a certificate of possession (of classified matter). The contracting officer must then transmit the certificate to the DOE cognizant security authority.
 - (1) Certificates of Non-Possession. Upon return or destruction of all classified matter pertaining to a contract, the contractor must submit a certificate of non-possession to the cognizant security authority. The certificate must include the contract number and a statement that all classified matter has been returned or destroyed (see Figure II-9).

(2) Certificates of Possession.

- (a) Requests to retain classified matter must indicate the benefit to DOE and the intended use of the information. Certificates must specifically identify classified matter by subject, type or form, and quantity (see Figure II-10).
- (b) If the classified matter will aid the contractor in performing another active Government contract and the matter is being transferred to the active contract, the contractor must provide the DOE cognizant security authority or the OGA holding the contract a copy of the retention notification. If the contractor is not notified to the contrary, the matter may be transferred and will fall under the jurisdiction of the gaining (i.e., active) contract.
- (c) When a certificate of possession is submitted, the contractor may maintain the classified matter for 24 months unless notified to the contrary by the DOE cognizant security authority or OGA.

c. Termination of Facility Clearance. Notwithstanding the provisions for retention outlined above, if a facility clearance is terminated for any reason, classified matter in the facility's possession must be returned to DOE or disposed of in accordance with instructions from the cognizant security authority. A certificate of non-possession must be completed as part of the clearance termination process. For prime contracts, DOE is the cognizant security authority. To accomplish the termination requirements, the cognizant security authority must ensure the following steps are accomplished.

- (1) determine whether a moratorium or ongoing litigation restricts actions;
- (2) acquire all classified matter not authorized for destruction.
- (3) conduct a 100 percent inventory of all accountable matter; taking appropriate action if any matter is missing;
- (4) check to ensure that all matter has been returned, if applicable.
- (5) destroy all copies, except record copies, of all classified documents.
- (6) send all remaining classified matter to the site specified by the responsible contracting officer and cognizant security authority.

Once the matter is destroyed or transferred, the cognizant security authority must complete the facility termination procedures (see DOE M 470.4-1, *Safeguards and Security Program Planning and Management*).

CERTIFICATE OF NONPOSSESSION OF CLASSIFIED MATTER

This letter/memorandum is to certify that to the best of (insert your company name)'s knowledge, we have destroyed properly or returned to authorized representatives of the Department of Energy (DOE) all classified matter used in connection with work performed for DOE under contract (insert contract, subcontract, or other agreement number/name).

Signature:

Date:

Title:

Company:

Figure II-9. Example Certificate of Non-possession of Classified Matter

CERTIFICATE OF POSSESSION OF CLASSIFIED MATTER

This letter/memorandum is to certify that to the best of (insert your company name)'s knowledge, with the exception of the items listed below, we have disposed of properly or returned to authorized representatives of the Department of Energy (DOE) all classified matter used in connection with work performed for DOE under contract (insert contract, subcontract, or other agreement number/name).

List of matter being retained: [Identify documents and material retained by type, date, classification, level, category (if RD or FRD), unique document numbers (if required), number of copies, length of retention, and any other pertinent data].

(Insert company name) understands and agrees to the following.

1. The listed documents will retain their present classification until downgraded or declassified by DOE and will be safeguarded in accordance with DOE security requirements.
2. Unauthorized disclosure of classified information is subject to criminal penalties, as provided for by the Atomic Energy Act of 1954; the Espionage Act; and other security directives.
3. Any unaccounted-for classified matter or potential compromise of the matter listed shall be reported immediately in accordance with DOE security requirements.

Signature:

Date:

Title:

Company:

Figure II-10. Example Certificate of Possession of Classified Matter

8. DESTRUCTION.

- a. Procedures must be established for the ongoing review of classified holdings to reduce volume to the minimum necessary. Multiple copies, obsolete matter, and

classified waste must be destroyed as soon as practical. Classified matter must be destroyed in accordance with records disposition schedules, including the NARA GRSs, and DOE records schedule.

- 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 DOE Office of General Counsel and appropriate records management organization.
- c. Classified matter must be destroyed beyond recognition to preclude subsequent access to any classified or sensitive information or other matter. (As one example, from an Operational Security perspective, destroyed material may produce sensitive residue that could provide a technological advantage to an adversary, or permit a forensic reconstruction.) Electronic storage media (ESM) must be destroyed in accordance with the DOE cyber security directives. Destruction techniques include burning, shredding, pulping, melting, mutilating, pulverizing, or by chemical decomposition. The following additional requirements must be satisfied when classified matter is destroyed.
 - (1) The DOE cognizant security authority must approve the use of public destruction facilities or any other alternative procedures (e.g., burying or disassembly).
 - (2) If classified matter cannot be destroyed onsite, it must be destroyed at a public destruction facility by a cleared individual on the same day it is removed from the site. A record of dispatch is not required unless custody of the matter is released to another cleared contractor or OGA.
 - (3) Ash residue produced by burning must be examined and reduced by physical disturbance to ensure that the matter is completely destroyed and no unburned matter remains.
 - (4) Classified microforms must be destroyed by burning, chemical decomposition, disintegration, or other methods approved by the cognizant security authority.
 - (5) Classified ESM destruction must include examination to assure that the media is no longer usable and that no classified information is present or recoverable. Formal certification, performance testing and accreditation of all associated technology, equipment and processes are required (reference DOE cyber security directives for additional destruction requirements). ESM that has been destroyed in this manner may be re-designated as unclassified and removed from accountability.
 - (6) For printing operations the “regaining” of reproduction plates is not an authorized method of destruction. Impressions of classified information

must be destroyed at the end of the run by cleaning the rollers and other parts of the presses to remove the classified information.

- (7) Some destruction methods may pose environmental hazards creating environmental concerns. In addition to obtaining DOE cognizant security authority approval to destroy classified matter by such methods, site personnel must determine whether approval is also required by Federal and State environmental protection agencies.
 - (8) For burial of classified matter, the primary concern is the likelihood of retrieval. When contemplating burial as a destruction option, the cognizant security authority must consider the following:
 - (a) if possible, reserve burial for non-paper matter only;
 - (b) the location within the burial grounds for classified matter;
 - (c) access controls;
 - (d) the difficulty of retrieval through some type of “entombment” process (e.g., encasement in concrete); and
 - (e) health and safety measures for contaminated classified matter.
- d. Equipment. Classified matter must be destroyed by equipment that has been approved by the cognizant security authority. The residue output must be inspected each time destruction is effected to ensure that established requirements have been met. Procedures must be established to ensure compliance with the manufacturer’s instructions, as appropriate, for operating destruction equipment and to ensure continuing effectiveness.
- (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 in width by 5 mm in length. (Note exception in following paragraph.)

Crosscut shredders purchased prior to December 31, 2003, that produce residue with a particle sizes not exceeding 1/32 of an inch in width by 1/2 inch in length 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 width by 1/2 inch maximum particle dimensions.

- (2) Pulping equipment must be equipped with security screens with perforations of 1/4 inch or smaller.
 - (3) Pulverizing equipment must be outfitted with security screens that meet the following specifications:
 - (a) Hammer mill perforations must not exceed 3/16 inch in diameter.
 - (b) Chopper and hybridized disintegrator perforations must not exceed 3/32 inch in diameter.
- e. Witnesses.
- (1) The destruction of classified matter must be accomplished by individuals who have appropriate access authorization for the classification level of the matter to be destroyed.
 - (2) The destruction of non-accountable classified matter may be accomplished by one individual; no witness is required.
 - (3) The destruction of accountable classified matter must be witnessed by an appropriately cleared individual other than the person destroying the matter. Locations with only one employee with appropriate access authorization must contact their cognizant security authority for guidance on destruction.
- f. Records of Destruction. Originators determine a document's disposition at the time of creation. Records must be maintained in accordance with NARA GRS 18 and the DOE records schedule.
- (1) Accountable Matter. 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. An audit trail must be maintained until destruction (see Figures II-11a and b).
 - (2) Non-accountable Matter. Non-accountable matter does not require destruction receipts or certificates.
 - (3) Disposition of Records. Destruction records must be maintained in accordance with both the NARA GRSs and the DOE records schedule. GRS 18 and DOE O 200.1, *Information Management Program*, dated 9-30-96, provide detailed information about records disposition.

DOE F 5635.9 (06-97) All Other Editions are Obsolete	U.S. DEPARTMENT OF ENERGY RECORD OF DESTRUCTION			OMB Control No. 1910-1800 OMB Burden Disclosure Statement on Reverse
See DOE M 470.4-4, <i>Information Security</i> , for instructions.				
UNCLASSIFIED DESCRIPTION OF MATTER (Subject or title and originator)	UNIQUE IDENTIFICATION NUMBER (If none, omit)	DATE OF MATTER	CLASSIFICATION LEVEL AND CATEGORY (Include any caveats)	NUMBER OF PAGES
I CERTIFY THAT THE MATTER LISTED ABOVE HAS BEEN DESTROYED IN ACCORDANCE WITH CURRENT SECURITY REGULATIONS.				
Signature, organization, and title of person destroying matter:			Date of Destruction:	
Signature, organization, and title of person witnessing destruction (if required):			Date of Destruction:	
v Printed with soy ink on recycled paper				

Figure II-11a. DOE F 5635.9, Record of Destruction

OMB Burden Disclosure Statement

Public reporting burden for this collection of information is estimated to average 5 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Information, Records, and Resource Management, HR-41- GTN, Paperwork Reduction Project (1910-1800), U.S. Department of Energy, 1000 Independence Avenue, SW., Washington, D.C. 20585; and to the Office of Management and Budget (OMB), Paperwork Reduction Project (1910-1800), Washington, DC 20503.

Figure II-11b. DOE F 5635.9, Record of Destruction, OMB Burden Disclosure Statement

- g. Classified Waste. Classified waste must be destroyed by approved methods as soon as practical. Receptacles used to accumulate classified waste must be clearly marked to indicate their purpose. Pending destruction, classified waste and receptacles must be protected as required for the level and category of classified matter involved.
- (1) Non-accountable classified matter (i.e., any matter classified as Secret or Confidential that is *not* entered into an accountability system) may be destroyed as classified scrap or waste. Examples of classified scrap or waste include typewriter, teletype, and dot matrix ribbons; notes, drafts, and working papers; carbon paper copies; X rays; imperfect copies of master documents; and any matter in excess of operational needs.
 - (2) Regardless of the method selected to store classified scrap pending destruction, certain considerations should be taken into account.
 - (a) Accountable matter should never be placed in containers (e.g., envelopes, files, and security container drawers) used as repositories for classified scrap.
 - (b) Containers should be emptied frequently enough to ensure that classified matter is destroyed within 180 days of origination.
9. FOREIGN GOVERNMENT INFORMATION PROGRAM. The requirements in this paragraph are provided in addition to other protection and control measures 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 is 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 (Table II-2 is a matrix of U.S. equivalent classification levels).

b. Release of U.S. Classified Information to Foreign Governments.

(1) National Disclosure Policy Committee (NDPC). The multi-agency NDPC, of which DOE is a “Special Member,” governs the export of classified military material and information 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 material provided to DOE. Before access to classified information is granted, several political agreements must be reached.

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. 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 (JAIEG) before disclosing atomic information (which includes RD and FRD) (Refer to O 470.4, *Safeguards and Security Program*, Section 5.c., Under Secretary for Nuclear Security/Administrator of the National Nuclear Security Administration, for additional details.) When the information proposed for disclosure contains classified military information, the disclosure must be approved in accordance with the National Disclosure Policy.

(2) Office of Health, Safety and Security. The Office of Health, Safety and Security is responsible for ensuring DOE’s compliance with National-level disclosure requirements such as those of the NDPC and the JAIEG. Before implementation, all agreements involving the disclosure of classified information to foreign governments and international agencies must be coordinated with the Office of Health, Safety and Security, which requires the following data regarding the information to be shared: 1) type of information; 2) justification for disclosure; 3) classification level and category (and caveats, if applicable); 4) originator (if not DOE); and 5) security considerations for protection.

(3) Prohibitions. Disclosure of classified information to foreign governments is not permitted where such disclosure is prohibited by law, Presidential orders, directives, international agreements, or other U.S. policy.

- (4) 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 United States. In making such a determination, the following conditions must be met:
- (a) The disclosure must be consistent with the foreign policy of the United States toward the receiving government.
 - (b) The disclosure must be consistent with the policies of the U.S. Government regarding either (a) the Atomic Energy Act of 1954, as amended, and the Energy Reorganization Act of 1974, or (b) information for which special procedures for release have been, or may hereafter be, established. Only a competent authority with statutory jurisdiction over the subject matter will establish these policies.
 - (c) The disclosure must be consistent with the National security interests of the United States.
 - (d) The disclosure must be limited to information necessary to the purpose for which disclosure is made.
 - (e) The receiving government must have agreed, either generally or in the particular case, to the following stipulations.
 - 1 The receiving government will not release the information to a third party without the approval of the releasing party.
 - 2 The receiving government will afford the information substantially the same degree of protection afforded the information by the releasing party.
 - 3 The receiving government will use the information *only* for the purpose for which it was given.
 - 4 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.
 - (f) In some instances, new documents may be created that contain both U.S. classified information and FGI. In these cases, unless there is a current agreement for cooperation covering RD or FRD, or an appropriate international agreement covering NSI which specifically allows the sharing of these levels and categories of classified information, the document may not be returned to the

originating government or international organization of governments.

(5) Release Determination.

- (a) Initiation and Coordination. The Departmental element responsible for the classified information to be released to a foreign government will prepare the initial request and justification. The Departmental element will coordinate with the Office of Health, Safety and Security, General Counsel, and the Congressional and International Affairs Office for approval to release the classified information.
- (b) Determination of Net Advantage to the U.S. The Deputy Administrator, Defense Nuclear Nonproliferation, in coordination with the General Counsel, the Office of Health, Safety and Security, and the cognizant Departmental element, and other program offices as necessary, must determine, as required by paragraph 9.b.(4), “that furnishing classified information will result in a net advantage to the national security of the United States.” The Deputy Administrator, Defense Nuclear Nonproliferation must consult with the Department of State and other agencies and departments, as appropriate, in making this determination.

(6) Exchange Agreements.

- (a) General. Before developing an exchange agreement, the Office of Health, Safety and Security must confirm the existence of an applicable government-to-government agreement between the United States and the foreign country or international agency involved.
- (b) Development of DOE Agreements. The Deputy Administrator, Defense Nuclear Nonproliferation, in coordination with the General Counsel, the Office of Health, Safety and Security, cognizant Departmental elements, and other program offices as necessary, must develop a classified information exchange agreement for each foreign government or international agency before: a) initial transfer of classified documents or material; or b) initial access to material in written or oral form.
- (c) Contents. Information-exchange agreements must specify the necessary requirements to ensure the security of the transferred documents, material, or information. They must be compatible with the terms and conditions of existing government-to-government agreements applicable to the transfer of classified information.

- (d) Execution of Agreements. DOE must execute an exchange agreement on a finding that the recipient government will provide adequate protection of the information to be furnished.
- (7) Transmittal of Classified Information. All transmittals of classified information must be made by DOE unless the contractor has prior written authorization.
 - (a) General. Except as identified in this Section, there are no additional requirements for the transmittal, receipt, or handling of classified information that is either received from, or sent to, foreign governments or international agencies.
 - (b) Review of Documents to be Transmitted.
 - 1 Classified documents or material to be transmitted to foreign governments must be forwarded to the Office of Health, Safety and Security for classification review.
 - 2 Classified documents or material to be transmitted to foreign governments must be forwarded to the Office of Health, Safety and Security for review to ensure that the information to be transmitted is within the scope of existing government-to-government agreements and legal concurrence has been obtained from General Counsel.
 - 3 If the transfer involves classified information or material produced by or received from another Government agency, the Office of Health, Safety and Security must obtain approval from the agency before transmission.
- (8) Preparation and Method of Transmission. The preparation, including classification markings and method of transmission of documents, must be the same as is prescribed in paragraph 9.c.(2) for the classification level of the information involved. Normally, documents intended for foreign governments will be forwarded to the receiving country's embassy in the United States. Transmission of classified mail to foreign countries requires the prior approval of the Director, Office of Health, Safety and Security.
- (9) Transmittal Documentation.
 - (a) Records on oral disclosures, made or contemplated, must be contained in memorandums prepared by the cognizant Departmental element and maintained by the Office of Health, Safety and Security.

- (b) A record of the information being processed for release must be maintained by the Office of Health, Safety and Security. The records must include the following:
- 1 identification of the exact information being released or being processed for release (for documents, give document date, title, names of originators, and classification);
 - 2 names and signatures of approving officials;
 - 3 form in which information is released or is to be released (oral, written, or material);
 - 4 date of release or contemplated release;
 - 5 identity of foreign government organization to which, and original individual recipient to whom, release is made or contemplated;
 - 6 security assurance or security check for each individual recipient;
 - 7 waivers exercised or requested, where applicable;
 - 8 statement that the information is based on data originated outside DOE, wherever applicable, and identity of originating organization; and
 - 9 citation of authority for release by an outside source, if applicable.
- c. Classified Information Received from Foreign Governments. To ensure the protection of classified FGI in accordance with Executive Order 12958, as amended, the following requirements must be met.
- (1) Handling. Classified information received from foreign governments and international agencies must be handled according to the requirements for classified matter set forth in this chapter. There are no additional handling requirements unless specifically identified in transfer agreements.
 - (2) Marking.
 - (a) Classified information from a foreign government must be marked in accordance with paragraph 3. (Table II-2 lists foreign classification-level markings).
 - (b) The front page of a document that contains FGI must include the marking, "This document contains (*indicate country of origin*)

information.” If the identity of the specific government must be concealed, the document must be marked, “This document contains foreign government information.”

- (c) When the identity of the specific government must be concealed, a separate record that identifies the foreign government must be maintained to facilitate subsequent declassification actions. When classified records are transferred to NARA for storage or archival purposes, the accompanying documentation must, at a minimum, identify the boxes that contain FGI. If the fact that the information is FGI must be concealed, the markings described in this paragraph must not be used, and the document must be marked as if it were wholly of United States origin.
- (3) Top Secret Foreign Government Information. The following requirements must be implemented for Top Secret FGI. Top Secret FGI must be:
 - (a) entered into accountability;
 - (b) reproduced only with the consent of the originating government; and
 - (c) witnessed upon destruction.
 - (4) Secret Foreign Government Information. The following requirements must be implemented for Secret FGI. Secret FGI:
 - (a) must be entered into accountability when required by treaties or international agreements;
 - (b) may be reproduced to meet mission requirements unless specifically prohibited by the originating government; and
 - (c) must be witnessed upon destruction.
 - (5) Confidential Foreign Government Information. Unless requested by the originating government, records are not required to be maintained for Confidential FGI.
- d. Confidential Foreign Government Information–Modified Handling Authorized (C/FGI-MOD). To ensure the protection of FGI provided in confidence, it must be classified under Executive Order 12958, as amended. If the foreign protection requirement is lower than the protection required for U.S. Confidential information, the following requirements must be met.
- (1) Marking. Documents may maintain their original foreign markings if the markings provide immediate recognition that the information requires special protection and control. Otherwise, FGI documents must be

- (2) reviewed by a derivative classifier, and if determined to be C/FGI-MOD, the first page of the document must include:
 - (a) the derivative classifier marking, and
 - (b) the statement, “This document contains (*name of country*) (*classification level*) information to be treated as U.S. Confidential-Modified Handling Authorized”.

If remarking is impractical, an authorized cover sheet (DOE F 470.9, C/FGI-MOD Confidential Foreign Government Information-Modified Handling Authorized) may be used (see Figure II-12).

- (3) Access/Need-to-Know. Access to C/FGI-MOD matter does not require DOE access authorization. However, such documents must be provided only to those who have an established need-to-know and where access is required by official duties.
- (4) Notification of Requirements. Individuals being given access to C/FGI-MOD matter must be notified of applicable handling instructions. This may be accomplished by a briefing, written instruction, or by applying the approved cover sheet.
- (5) Protection. C/FGI-MOD matter must be protected in the following manner.
 - (a) 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.
 - (b) Protection in Storage. C/FGI-MOD matter must be stored to preclude unauthorized disclosure. When not in use, such matter must be stored in locked receptacles (e.g., file cabinets, desks, or bookcases) accessible only by persons who have a need-to-know the C/FGI-MOD information contained in the matter. Open storage is allowed if every person with access to the room or building also has a need-to-know the C/FGI-MOD information contained in the matter; however, the room or building must be locked when no one is present.
- (6) 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. The reproduced matter must be marked and protected in the same manner as the original matter. Copy machine malfunctions must be cleared and all paper paths checked for

C/FGI-MOD material. Excess paper containing C/FGI-MOD matter must be destroyed as described below.

DOE F 470.9
(08/2005)
All Other Editions Are Obsolete

U.S. DEPARTMENT OF ENERGY

C/FGI-MOD

CONFIDENTIAL FOREIGN GOVERNMENT INFORMATION - MODIFIED HANDLING AUTHORIZED -

As defined by Executive Order 12958, Section 1.1(3), "Foreign Government Information" means:
(1) information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both are to be held in confidence;
(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or
(3) information received and treated as "Foreign Government Information" under the terms of a predecessor order.

The attached document contains *Foreign Government Information (FGI)*, as defined by Executive Order 12958, "Classified National Security Information," that the foreign government protects at a level lower than U.S. CONFIDENTIAL.

Access to the attached information does not require an access authorization or personnel security clearance. However, access to this information must only be granted to persons with an established need to know and whose official duties require access. This information must not be disclosed to a third party government, individual, group, or organization not involved in the applicable agreement or treaty without the expressed, written permission from the originator.

When not in use, this document must be stored in a locked receptacle (e.g., file cabinet, desk, bookcase) that is accessible only by persons who have a need to know the information to perform their official duties to ensure protection against unauthorized disclosure or access by unauthorized personnel.

***This Cover Sheet May Be Applied To All Qualified FGI Documents
While Under U.S. Control in U.S. Facilities.***

C/FGI-MOD

This document contains _____ information
(Insert name of country)

18 U.S.C. SECTION 1010; ACT OF JUNE 25, 1948; 62 STAT 748; MAKES IT A CRIMINAL OFFENSE TO MAKE A WILLFULLY FALSE STATEMENT OR REPRESENTATION TO ANY DEPARTMENT OR AGENCY OF THE UNITED STATES AS TO ANY MATTER WITHIN ITS JURISDICTION.

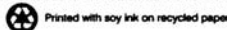


Figure II-12. DOE F 470.9, C/FGI-MOD Confidential Foreign Government Information-Modified Handling Authorized

Vertical line denotes change.

- (7) Destruction. When C/FGI-MOD matter is to be destroyed, it must be sufficiently destroyed to preclude any of the information it contained from being recovered. At a minimum, C/FGI-MOD matter must be destroyed by using strip cut shredders that result in particles of no more than ¼-inch wide strips. Methods that are approved for destruction of classified matter may be used. Other methods that provide sufficient destruction may be approved by the DOE cognizant security authority. The decision to dispose of any DOE matter, whether or not it contains C/FGI-MOD matter, must be consistent with the policies and procedures for records disposition.
- (8) Transmission. C/FGI-MOD matter must be transmitted by means that preclude unauthorized disclosure or dissemination.
- (a) Outside a Facility.
- 1 Matter marked as containing C/FGI-MOD matter must be packaged in a single, opaque envelope or wrapping.
 - 2 Any of the following U.S. mail methods may be used to transmit C/FGI-MOD: U.S. First Class, Express, Certified, or Registered Mail.
 - 3 C/FGI-MOD matter may be transmitted by any commercial carrier.
 - 4 C/FGI-MOD matter may be hand-carried as long as strict control can be maintained at all times.
- (b) Within a Facility.
- 1 A single opaque, sealed envelope should be used. A standard distribution envelope such as the U.S. Government Messenger envelope (SF 65-B) or equivalent may be used to transmit C/FGI-MOD provided the information is not visible outside the envelope.
 - 2 C/FGI-MOD matter may be hand-carried as long as strict control can be maintained at all times.
- (c) Over Telecommunications Circuits. If using telecommunications services, including voice (telephonic, point-to-point), facsimile, narrative message, communications facilities, and radio communications, organizations must employ the most secure method readily available for the transmission of C/FGI-MOD matter. Factors to consider when deciding what method to use

will include, but not be limited to; physical, personnel, administrative, communications protective features, and any other supplemental controls established to provide an acceptable level of protection for C/FGI-MOD matter. These protective features must deter access to C/FGI-MOD matter by unauthorized individuals and restrict public releasability.

If C/FGI-MOD matter is transmitted over public switched-broadcast communications paths (e.g., the Internet), the information must be protected by encryption. This may be accomplished through DOE public key systems or encryption algorithms that comply with all applicable Federal laws, regulations, and standards addressing the protection of classified and other unclassified controlled information (see chapter 9 of DOE M 200.1-1, *Public Key Cryptography and Key Management*, dated 2/15/00). In emergency situations, the cognizant security authority may waive encryption requirements.

- (d) Automated Information Systems. The automated information system or automated information system network must ensure that only personnel who are authorized for access to C/FGI-MOD matter can access that information. For instance, networks inter-connected with a public switched-broadcast network (e.g., the Internet) must provide precautions (e.g., authentication or file access controls) to ensure that C/FGI-MOD matter is protected against unauthorized access. C/FGI-MOD matter being transmitted over broadcast networks like the Internet, where unauthorized access is possible, must provide protection (e.g., encryption) to ensure that the information is not improperly accessed.
- e. 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 access authorization and meet need-to-know requirements.
- f. Third-Country Transfers. The release or disclosure of FGI to any third-country entity must be coordinated through the cognizant Departmental element and 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.
- g. Foreign Government Information Containing Unclassified U.S. Information. Documents containing U.S. unclassified information and FGI must be protected at the level of the FGI.

- h. Return of Foreign Government Information Containing Classified U.S. Information. U.S. classified information may be added to a document containing FGI (e.g., through analysis by U.S. experts). In this case, unless there is a current agreement for cooperation (for RD or FRD) or appropriate international agreement (for NSI) 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. If it is necessary to provide the enhanced FGI back to the originating government or international organization, it must be handled in accordance with 9b above.

10. MATERIAL.

a. Marking.

- (1) Requirements. Paragraphs 3.c.(5) and 3.d.(3) require that classified material have the classification level and category (if RD or FRD) stamped, printed, etched, written, engraved, or painted on or affixed to it by means of tag, sticker, decal, or similar device. When marking is not practical, written notification of the markings must be furnished to recipients.
- (2) 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 verified as compatible with the material being marked.
- (3) 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 material. Other markings such as originator identification and unique identification number (accountable material only) do not apply because of the nature of the material.

b. Alternatives to Standard Markings.

- (1) General. Requirements in this Section must be followed to the maximum extent possible. Alternative procedures for marking classified materials where standard markings are not possible must be approved by the cognizant security authority.
- (2) Abbreviations. If the part, tool, gauge, or material is too small to carry the full category stamp, it may be marked with only the classification level and category (if RD or FRD) or its abbreviation (S/RD, C/FRD, etc.).

- (3) Tagging. Classified material may be marked by attaching a tag containing the appropriate information.
- (4) Stickers/Decals/Labels. Classified material may be marked by affixing a sticker, decal, or label directly on it, as long as this technique does not violate engineering, war reserve, or configuration control requirements.
- (5) Bagging. Classified material may be marked by placing it in a bag and applying to the bag a decal, label, or sticker containing the required information.
- (6) Placard or Notice. A placard or notice containing the required information may be maintained near material that cannot be marked directly. This technique is likely to be used when parts are stored and worked on in inaccessible places like glove boxes.
- (7) Other Means. If marking the material itself is impractical, the wrapper, container, tray, bin, or cart may be marked with the appropriate classification level and category (if RD or FRD) information.

c. Accountability Requirements.

- (1) General. Accountability requirements also must be adjusted to accommodate the physical characteristics of the material. Accountability procedures must be approved by the cognizant security authority.
- (2) Exemptions. When they are *not* applicable, the following items are exempt from inclusion in the material accountability records:
 - (a) matter date;
 - (b) number of copies; and
 - (c) date and disposition of reproduction.
- (3) Requirements. The material accountability system must provide a description of each type of item, the classification level and category (if RD or FRD), the number of items of each type, and scheduled inventories. Part numbers and serial numbers should be used, when available, either to assist with unique numbers or identify types of material. Where applicable, the production cycle and production control procedures can be used to facilitate the conduct of all inventories of accountable material.

CHAPTER III. PROTECTION OF CLASSIFIED MATTER

1. GENERAL REQUIREMENTS.

- a. Classified matter is any combination of data, documents, and material containing classified information. This includes classified parts and explosives whose shape are considered classified. Requirements for protecting classified special nuclear material (SNM) are found in other Department of Energy (DOE) directives (see DOE M 470.4-2, *Physical Protection* and DOE M 470.4-6, *Nuclear Material Control and Accountability*).
- b. Classified matter must be processed, handled, or stored in security areas providing protection measures equal to or greater than those in a Limited Area (LA). Secret matter that cannot be processed, handled, and/or stored within an LA or higher must be maintained in an accountability system, as described in Chapter II of this Section, in addition to having intrusion detection systems and protective force (PF) response, as required by paragraph 2., below. Need-to-know controls, appropriate physical security, and access control measures must be applied to each area or building within a security area where classified matter is handled or processed.
- c. Commingling Classified Matter.
 - (1) Classified and unclassified documents may be commingled. For example, Top Secret (TS), Confidential (C), and unclassified documents may be stored in the same file folder. Need-to-know considerations, however, might make it necessary to segregate documents (e.g., to avoid photographing Top Secret documents onto the same reel or microfiche as Secret (S) or Confidential documents). Good business practice suggests marking commingled unclassified documents as "Unclassified" when storing/filing with classified documents.
 - (2) Classified Removable Electronic Media (CREM) that contain Sigma 1, 2, 14, or 15; a combination of nuclear weapons design/test data; or Top Secret or Special Access Program (SAP) matter must be separated from and not commingled with other classified information/media. This may be accomplished using file folders or similar methods.

2. STORAGE REQUIREMENTS. The following physical security storage requirements apply to classified safeguards and security (S&S) interests.

- a. Restrictions on Security Containers Used for Classified Matter.
 - (1) Funds, firearms, medical items, controlled substances, precious metals, or other items susceptible to theft must not be stored in the same storage container used to store classified matter.

- (2) Security containers 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. Security Container Requirements. Security containers used for storing classified matter must conform to General Services Administration (GSA) standards and specifications. Vaults and vault-type rooms (VTRs) used for open storage of classified matter must meet the requirements of DOE M 470.4-2, *Physical Protection*.
- (1) Classified matter that is not under the personal control of an individual with appropriate access authorization and need-to-know must be stored as described below.
 - (a) If inspections by PF personnel are used as supplemental control, PF personnel must examine exposed surfaces of the security container, vault, VTR, and steel filing cabinets for evidence of any forced entry to ensure that the security container or door is locked and the Standard Form (SF) 702 completely annotated.
 - (b) The classified matter must be protected by means to detect unauthorized access.
 - (c) Areas and buildings must be protected from adversary access by application of locks and barriers. Requirements for these locks and barriers can be found in DOE M 470.4-2, *Physical Protection*.
 - (2) 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.
 - i. If the container is located in an LA, Exclusion Area (EA), Protected Area (PA), or Materials Access Area (MAA), the GSA-approved security container must have a lock meeting Federal specification FF-L-2740A, "Locks, Combination."
 - (b) In a locked vault or VTR within an LA, EA, PA, or MAA. The vault or VTR must be equipped with intrusion detection

equipment, and PF personnel must respond within 15 minutes of alarm annunciation.

- (c) In a locked vault or VTR outside an LA, EA, PA, or MAA that must be under intrusion detection system protection. The PF must respond within 5 minutes of alarm annunciation.
- (3) Secret matter must be stored in a manner authorized for Top Secret matter or as described below.
- (a) In a locked vault (requirements for vaults are included in DOE M 470.4-2, *Physical Protection*); or in a locked GSA-approved security container within an LA or higher.
 - (b) In a locked VTR (requirements for VTRs are included in DOE M 470.4-2, *Physical Protection*) within an LA, EA, PA, or MAA equipped with intrusion detection system protection. The PF must respond within 30 minutes of alarm annunciation.
 - (c) When located outside an LA, the locked vault or VTR must be under intrusion detection system protection. The PF must respond within 15 minutes of alarm annunciation.
 - (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 an LA, EA, PA, or MAA. 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 when the area is unattended.
 - 2 Inspection every 4 hours by PF or by cleared duty personnel when unattended.
- (4) Confidential matter must be stored in the same manner prescribed for Top Secret or Secret matter, but the supplemental controls are not required.
- (5) Complete nuclear weapon configurations, nuclear test and trainer devices, and nuclear-explosive-like assemblies without nuclear material must be stored in a vault or VTR located, at a minimum, within an LA. PF personnel must respond within 15 minutes of alarm annunciation.
- c. Response Personnel. Protective personnel, private security firms, or local law enforcement agency personnel must respond to intrusion detection system alarms

as specified in paragraph 2.b. above. Specific details regarding this response (e.g., numbers of personnel responding, response positions, and duties) must be described in an approved site safeguards and security plan or site security plan.

d. Alternative Storage Locations.

- (1) With prior written approval of the cognizant security authority, a bank safe deposit box/vault may be used to store Secret or Confidential matter, provided that the lock and keys to the box/vault are changed before such use and the customer's key is furnished only to persons authorized access to the contents. The key must be stored in locked container.
- (2) Approved Federal Records Centers may be used to store classified information (see DOE M 470.4-1, *Safeguards and Security Program Planning and Management*).

SECTION B—OPERATIONS SECURITY

1. OBJECTIVES.

- a. To help ensure that Critical Program Information (CPI), including unclassified controlled information 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 Department.

2. REQUIREMENTS.

- a. An OPSEC program must be implemented to cover each program office, site, and facility to ensure the protection of classified and unclassified controlled information. The OPSEC program, in addition to ensuring the compliance with the requirements of this Manual, 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 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 national and departmental requirements and may be integrated into, or provided in conjunction with, required security briefings (e.g., new hires' initial briefings, comprehensive or annual refresher briefings).
 - (4) Participation in self-assessments to ensure the national, departmental, and local requirements to protect and control classified and unclassified controlled information 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 Office of Health, Safety and Security and to the Associate Administrator for Defense Nuclear Security when involving National Nuclear Security

Administration (NNSA) facilities, in a timely fashion, to include implementation and expiration of such actions.

- (6) Promulgation of new OPSEC requirements to all affected employees.
 - (7) Interaction and coordination with 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 Office of Health, Safety and Security is through the Associate Administrator for Defense Nuclear Security.
- b. OPSEC plans must be developed for programs and operations and approved by the cognizant security authority.
 - 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 SAP information within their boundaries. OPSEC assessments must be conducted at other facilities involved in creating, handling, storing, processing, or transmitting CPI, as deemed necessary by the cognizant security authority.
 - (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. The frequency of OPSEC assessments must be described in the OPSEC plan and conform to requirements set forth in National Security Decision Directive 298 and the National Industrial Security Program Operating Manual.
 - (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. Priority for conducting assessments will be based on CPI,

threat assessments, risk management principles, recommendations received from the local OPSEC working group, and direction from DOE line management.

- f. OPSEC 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.
 - (1) OPSEC reviews of sensitive activities and facilities must be conducted whenever the following criteria are met.
 - (2) New construction is planned for a facility that will process or store classified or sensitive information or matter.
 - (3) New sensitive activities are initiated or existing programs incur significant changes.
 - (4) 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 web sites.
 - (1) Before any information generated by or for the Federal Government (Government Information) is placed on a DOE, DOE contractor or sub-contractor web site or is otherwise made available to the public, it must be reviewed to ensure that it does not contain classified, unclassified controlled information or critical program information. Before DOE employees, DOE contractors, or sub-contractors post Government Information to a personal or non-DOE web site 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 DOE, 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 Departmental Elements must document a program element position which 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 Departmental 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 (SAPs) 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 Departmental 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 471.2-3A, *Special Access Program Policies, Responsibilities and Procedures*, dated 7-11-02.
 - b. Departmental SAPs must be limited to acquisition, operations, support, and intelligence activities.
 - c. Department of Energy (DOE) and non-DOE (Work for Others) SAPs, with the exception of intelligence SAPs, must be registered manually through the established Facility Clearance process using DOE F 470.2, Facility Data Approval Record (FDAR). For additional information regarding the FDAR process see DOE M 470.4-1, *Safeguards and Security Program Planning and Management*. The FDAR must be classified in accordance with current classification guidance. Departmental SAPs must be manually registered with the SAP Security Program Manager. Intelligence SAPs must be manually registered with the Office of Intelligence. Registration of all Intelligence SAPs, other than those housed in a SCIF, will be coordinated between the DOE SAP Security Program Manager and the Intelligence Work for Others Coordinator.
 - d. SAP facilities, work areas, and activities must be surveyed according to DOE M 470.4-1, *Safeguards and Security Program Planning and Management* by the cognizant SAP Security Coordinator in coordination with the cognizant program office and/or sponsor. Intelligence SAPs must be surveyed by the Office of Intelligence in conjunction with the Sponsor. Independent oversight inspections must be performed for Departmental programs in accordance with DOE M 471.2-3A.
 - 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, *Safeguards and Security Program Planning and Management*, contains additional requirements.)

SECTION D—UNCLASSIFIED CONTROLLED INFORMATION

1. OBJECTIVES. To adequately and consistently control and protect unclassified controlled information (UCI) within the Department. UCI is broadly defined as unclassified information that may be exempt from public release under the Freedom of Information Act and for which disclosure, loss, misuse, alteration, or destruction may adversely affect national security, governmental interests, or personal privacy.
2. REQUIREMENTS. UCI is protected through marking, access control, physical protection, and other requirements for reproduction, transmission, destruction, and dissemination. Such information, and associated protection requirements include, but are not limited to.
 - a. Other Agency Controlled Information. Unclassified controlled information created by other agencies. Examples include State Department information known as “Sensitive but Unclassified” (SBU) and Department of Defense information known as “For Official Use Only” (FOUO). Protection requirements for this type of information are established by the originating agency. When the originating agency requirements cannot be obtained, documents bearing these markings are protected within DOE as Official Use Only (OUO) information (see DOE M 471.3-1, chapter II).
 - b. Unclassified Controlled Nuclear Information (UCNI). Certain unclassified but sensitive information concerning nuclear material, weapons, and components the distribution of which is controlled under section 148 of the Atomic Energy Act. Detailed identification and protection requirements are contained in DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, dated 6-30-00, and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, dated 10-23-01.
 - c. Official Use Only (OUO). Certain unclassified information that may be exempt from release under the FOIA. Detailed identification and protection requirements are contained in DOE O 471.3, *Identifying and Protecting Official Use Only Information*, dated 4-9-03, and DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, dated 4-9-03.
 - d. Naval Nuclear Propulsion Information (NNPI). Refer to Section A, Chapter II, 3.1.(5) for specific references.

SECTION E—TECHNICAL SURVEILLANCE COUNTERMEASURES

This Section is Official Use Only

Please contact the DOE Office of Health, Safety and Security
at 301-903-0292 to request a copy of Section E

APPENDIX 1. POSITIVE CONTROL OF REPOSITORY ACCESS WITH XO-SERIES LOCKS

For those containers equipped with X-07, X-08 or X-09 (XO series) locks, the XO series repository locks may be used in place of seals on containers located outside a vault or vault-type room (VTR). These locks possess a feature that affords built-in accountability by recording the number of openings. The number cannot be reset or modified manually and the counter resets automatically after 9999 openings. Also, when queried by a supervisor or custodian, these locks will reveal on the Liquid Crystal Display (LCD) the number of unsuccessful attempts at opening the lock between actual openings when that number exceeds three. The combination to the lock is not required to conduct these audits; therefore, after-hours checks can be accomplished by anyone that possesses physical access to the lock. For additional information, please refer to the following.

To mitigate the requirement for the use of seals on containers equipped with XO series locks, local procedures must include at least the following elements:

- Prior to opening the container, the authorized opener will operate the lock so as to display the number of prior openings. The number indicated should correspond to that noted on the Standard Form (SF) 702 for the previous opening. (If the number of openings has advanced by one or more integers, the custodian/alternate will report that the container lock had been opened with no SF 702 annotation.)
- The number of repository openings will be noted sequentially with other entries on the SF 702 with the date and time of the opening and the opener's initials. Each opening number, as recorded on the XO series lock, must be logged on the SF 702, along with the other required information, to provide a complete and up-to-date record of who opened the repository and when they did so. The lock opening numbers will be recorded for each repository on an SF 702. The new number (previous total plus one) will be noted on the SF 702 when opening the container, along with the associated date, time and opener's initials.

Repository access for containers with XO series locks are still limited to trained custodians and alternate custodians and all such General Services Administration (GSA)-approved repositories must be maintained within Limited Areas or higher. They must remain locked except when Accountable Classified Removable Electronic Media or other matter is being retrieved or returned. Weekly inventories must be conducted when these containers are located outside a vault or VTR.

Security Container Lock Opening/Closing Procedures

For Accountable Classified Removable Electronic Media (ACREM)


(Opening and Closing Only by Authorized ACREM Custodians or Appointed Alternates)



X-07 Combination Locked Containers

- **Opening Procedures:** (Note: Prior to beginning the lock opening process, ensure the LCD display on the lock is blank AND that the dial has not been turned in either direction for at least two minutes)

NOTE 1: The first time the X-07 lock is established as a re-useable electronic accountable seal, a reading of the “start-up” number of openings will be performed as in Step 2, below. This four digit number will be entered on an unused *Standard Form 702 (SF 702)* as the first entry on the first line by indicating the date and XO audit number, and signed on that line by the ACREM custodian or alternate. The first opening of the container will be recorded on the second line and will be the next number in sequence. All *SF 702s* must be labeled at the top of the form with the annotation of “ACREM.” (See attached *SF 702 for ACREM Containers* example.)

NOTE 2: The *SF 702* must be maintained in accordance with NARA requirements for receipts for classified matter (two years for Secret protected matter, and five years for Top Secret).

1. ***Examine*** the *SF 702* for the last recorded opening number (see column marked *Guard Check* for the container to be opened).
2. ***Dial*** the lock **CLOCKWISE** (Right)  until a display is visible in the dial window. **STOP**. Read the two sets of two-each flashing numbers beginning with the set of numbers with the arrow pointing left; then the set of numbers with the arrow pointing right. (Example: left arrow reads 12; right arrow reads 34. The composite number is 1234.) There will always be four, and only four digits displayed. If you have, in error, dialed in the counterclockwise (left) direction first, **STOP**, wait for the display to disappear, then wait at least two more minutes before restarting this procedure with step 1, above.
3. ***Compare*** this number you are reading with the last recorded opening number (column marked *Guard check*) on the *SF 702*. If these numbers do not match, **STOP**, and summon your local security office. **DO NOT ATTEMPT TO DIAL THE COMBINATION.** If the numbers match, continue to step 4, below.

4. **Warning:** Do not execute this step unless the three steps above have been completed with matching XO audit numbers. Within 40 seconds of previous dial movement, reverse dialing directions and dial **COUNTERCLOCKWISE (Left)**  to begin the combination dialing process. If, during the first turn to the left a “lightning bolt” and a number appears, **STOP**, and read the two digit number displayed with the lightning bolt. This number indicates that there have been “x” (≥ 3 but ≤ 99) unsuccessful opening attempts. Make a note of this number and report it as soon as possible to your local security office. The number of unsuccessful opening attempts will reset to “0” upon the first successful opening. Continue turning **COUNTERCLOCKWISE (Left)**  and dial the opening combination. Open the container.
5. Before proceeding, immediately **annotate** the *SF 702* with the date, time, your initials (ACREM Custodian/Alt), and the next in sequence opening number (column marked *Guard Check*) in the appropriate spaces. (Example: The last opening sequence number was 0967. You have verified, as above in steps 2 and 3, that the lock reads 0967. You now enter 0968 as the next opening sequence number.)

- **Closing Procedures**

1. **Close** the container. Turn the combination lock dial one full turn in the counterclockwise direction. Then turn the combination lock dial at least one full turn in the clockwise direction to ensure the lock is locked. (Note: if the dial stops and cannot be turned in the clockwise direction, the lock is not locked. Repeat this step.) Attempt to open the locking drawer and all other drawers with the lock in the locked mode.
2. **Annotate** the *SF 702* with the time and initials of an ACREM Custodian locking the container. A “double check” is required at the end of the working day. The person double checking the locked container does not need to be an ACREM custodian, but must ensure the container is locked by turning the combination lock dial at least one full turn in the clockwise direction and attempting to open the container. The checking individual must annotate the *SF 702* in the “checked by” column with the time and initials of the person performing the double check.

SF 702 for CREM Containers

CREM SECURITY CONTAINER CHECK SHEET									
FROM		ROOM NO.		BUILDING		CONTAINER NO.			
		A-201		GTN		S-12345			
CERTIFICATION									
I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.									
MONTH/YEAR									
08-2004									
DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)		
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	
09	Start-up		Signature of CREM Custodian/ALT				1797		
10	AL	8:06a	AL	8:10a			1798		
10	BR	9:20a	BR	9:25a	TV	5:07p	10:05p	GF	
11							2:01a	GF
11	AL	8:29a	AL	8:35a			6:11a	GF	
11	BR	4:50p	BR	4:55p	CT	5:14p	11:30p	GF	

Example

CREM Custodian/Alt
CREM Custodian/Alt
Anyone

NEW! XO Audit or Seal Number

Guard Check (if/when required)

NOTICE: Maintain this record in accordance with NARA requirements for receipts for classified matter (two years for Secret protected matter, and five years for Top Secret).

- 09 Container initialized with XO audit number (1797) and signature of CREM Custodian.
- 10 Audit number (1797) verified. Container opened at 8:06am by "AL." Next sequential number entered as opening number (1798).
- 10 Container closed at 8:10am by "AL."
- 10 Audit number (1798) verified. Container opened at 9:20am by "BR." Next sequential number entered as opening number (1799).
- 10 Container closed at 9:25am by "BR."
- 10 End of Day container check conducted at 5:07pm by "TV."
- 10 Guard check conducted at 10:05pm by "GF" (only performed if/when required).
- 11 Guard check conducted at 2:01am by "GF" (only performed if/when required).
- 11 Guard check conducted at 6:11am by "GF" (only performed if/when required).
- 11 Audit number (1799) verified. Container opened at 8:29am by "AL." Next sequential number entered as opening number (1800).
- 11 Container closed at 8:35am by "AL."
- 11 Audit number (1800) verified. Container opened at 4:50pm by "BR." Next sequential number entered as opening number (1801).
- 11 Container closed at 4:55pm by "BR."
- 11 End of Day container check conducted at 5:14pm by "CT."
- 11 Guard check conducted at 11:30pm by "GF" (only performed if/when required).

X-07 Abbreviated Procedures

(Note: Use only as a guide when detailed instructions are completely understood)

OPENING

1. Ensure there has been no lock dialing activity for 2 minutes after display has “blanked.”
2. Rotate lock dial clockwise (right) to power up lock and read the flashing “left arrow” / “right arrow” numbers displayed.
3. Compare this composite number with the last number entered (see column marked *Guard Check*) on the *SF 702*. If no match, **STOP**, and summon your local security office.
4. Dial counterclockwise (left). If a “lightning bolt” appears, stop and note the number to be reported to your local security office at your next opportunity. Continue dialing counterclockwise and proceed to open the lock.
5. Enter date, time, initials of a CREM custodian, and next sequential opening on the *SF 702*.

CLOSING

1. Close and lock the container, ensuring lock dial has been turned one full turn in the counterclockwise direction.
2. Check to ensure lock is locked by rotating lock dial one full turn in the clockwise direction.
3. Check each drawer by attempting to open each drawer.
4. Annotate the *SF 702* with time and initials of a CREM Custodian closing the container.
5. At end of work day, obtain the assistance of another person to check the security condition of the container by performing steps 2 and 3, above. Annotate the *SF 702* in the “checked by” column. The person checking need not be a CREM custodian.

20040809

Security Container Lock Opening/Closing Procedures

For Accountable Classified Removable Electronic Media (ACREM)


(Opening and Closing Only by Authorized ACREM Custodians or Appointed Alternates)

X-08 Combination Locked Containers



- **Opening Procedures:** (Note: Prior to beginning the lock opening process, ensure the LCD display on the lock is blank AND that the dial has not been turned in either direction for at least 15 seconds.) This lock is differentiated from the X-07 lock by a dial that stands out from the container mounting surface by 1½ times and is usually black in color.

NOTE: The first time the X-08 lock is established as a re-useable electronic accountable seal, a reading of the “start-up” number of openings will be performed as in Step 2, below. This four digit number will be entered on an unused Standard Form 702 (*SF 702*) as the first entry on the first line by indicating the date and XO audit number, and signed on that line by the ACREM custodian or alternate. The first opening of the container will be recorded on the second line and will be the next number in sequence. All *SF 702s* must be labeled at the top of the form with the annotation of “ACREM.” (See attached *SF 702 for ACREM Containers* example.)

NOTE 2: The *SF 702* must be maintained in accordance with NARA requirements for receipts for classified matter (two years for Secret protected matter, and five years for Top Secret).

1. ***Examine*** the *SF 702* for the last recorded opening number (see column marked *Guard Check* for the container to be opened).
2. ***Dial*** the lock **CONTINUOUSLY COUNTERCLOCKWISE** (Left)  until a display is visible in the dial window. (NOTE: Continuously counterclockwise normally requires two-handed operation such that dialing must not be paused or stopped during this process—dialing may require up to 25 turns.) **STOP**. Read the two sets of two-each flashing numbers beginning with the set of numbers with the arrow pointing left; then the set of numbers with the arrow pointing right. (Example: Left Arrow reads 12; right arrow reads 34. The composite number is 1234.) There will always be four, and only four digits displayed. If you have, in error, dialed in the clockwise (right) direction first, **STOP**, wait for the display to disappear, then wait at least 15 seconds before restarting this procedure with step 1.
3. ***Compare*** this number you are reading with the last recorded number (column marked *Guard Check*) on the *SF 702*. If these numbers do not match, **STOP**,

and summon your local security office. **DO NOT ATTEMPT TO DIAL THE COMBINATION.** If the numbers match, continue to step 4, below.

4. **Warning:** Do not execute this step unless the three steps above have been completed with matching XO audit numbers. Wait until the lock has powered down (display disappears). Wait at least 15 seconds before proceeding. Dial **COUNTERCLOCKWISE** (Left)  (not continuous) to power up lock. If, during this power up process to the left, a “lightning bolt” appears, **STOP**, and read the two digit number displayed with the lightning bolt. This number indicates that there have been “x” (≥ 3 but ≤ 99) unsuccessful opening attempts. Make a note of this number and report it as soon as possible to your local security office. (Note: If an “SA” indicator appears in the lock window at any time, you will not be able to open the lock. It indicates the lock has been attempted to be opened in excess of 15 times. You must contact your HSO to report the situation and obtain technical assistance.) The number of unsuccessful opening attempts will reset to “0” upon the first successful opening. Within 15 seconds, reverse direction and dial the lock combination in a CLOCKWISE “all right”  direction. Open the container.
5. Before proceeding, immediately **annotate** the *SF 702* with the date, time, your initials (ACREM Custodian/Alt), and the next in sequence opening number (column marked *Guard Check*) in the appropriate spaces. (Example: The last opening sequence number was 0967. You have verified, as above in steps 2 and 3, that the lock reads 0967. You now enter 0968 as the next opening sequence number.)

- **Closing Procedures**

1. **Close** the container. Turn the combination lock dial one full turn in the counterclockwise direction. Then turn the combination lock dial at least one full turn in the clockwise direction to ensure the lock is locked. (Note: if the dial stops and cannot be turned in the clockwise direction, the lock is not locked. Repeat this step.) Attempt to open the locking drawer and all other drawers with the lock in the locked mode.
2. **Annotate** the *SF 702* with the time and initials of the ACREM Custodian locking the container. A “double check” is required at the end of the working day. The person double checking the locked container does not need to be an ACREM custodian, but must ensure the container is locked by turning the combination lock dial at least one full turn in the clockwise direction and attempting to open the container. The checking individual must annotate the *SF-702* in the “checked by” column with the time and initials of the person performing the double check.

X-08 Abbreviated Procedures

(Note: Use only as a guide when detailed instructions are completely understood)

OPENING

1. Ensure there has been no lock dialing activity for 15 seconds after display has “blanked.”
2. Rotate lock dial **continuously counterclockwise** (left) to power up lock and read the flashing “left arrow” / “right arrow” numbers displayed.
3. Compare this number with the last number entered (see column marked *Guard Check*) on the *SF 702*. If no match, **STOP**, and summon your local security office.
4. Wait at least 15 seconds after lock display has disappeared. Dial counterclockwise (left). If a “lightning bolt” appears, stop and note the number to be reported to your local security office at your next opportunity. (Note: If “SA” appears in the dial window at any time, you will need to contact your local security office to obtain technical assistance.) Continue dialing clockwise (right) within 15 seconds, entering all combination numbers to the right, and proceed to open the lock.
5. Enter date, time, CREM Custodian initials, and next sequential opening number on the *SF 702*.

CLOSING

1. Close and lock the container, ensuring dial has been turned one full turn in the counterclockwise direction.
2. Check to ensure lock is locked by rotating lock dial one full turn in the clockwise direction.
3. Check each drawer by attempting to open each drawer.
4. Annotate the *SF 702* with time and initials of the CREM custodian closing container.
5. At end of work day, obtain the assistance of another person to check the security condition of the container by performing steps 2 and 3, above. Annotate the *SF 702* in the “checked by” column. The person checking need not be a CREM custodian.

Security Container Lock Opening/Closing Procedures

For Accountable Classified Removable Electronic Media (ACREM)


(Opening and Closing Only by Authorized ACREM Custodians or Appointed Alternates)

X-09 Combination Locked Containers



- **Opening Procedures:** (Note: Prior to beginning the lock opening process, ensure the LCD display on the lock is blank AND that the dial has not been turned in either direction for at least two minutes.) This lock is differentiated from the X-07 lock by a dial that stands out from the container mounting surface by 1½ times, and is normally gray in color.

NOTE: The first time the X-09 lock is established as a re-useable electronic accountable seal, a reading of the “start-up” number of openings will be performed as in Step 2, below. This four digit number will be entered on an unused SF 702 as the first entry on the first line by indicating the date and seal number, and signed on that line by the ACREM custodian or alternate. The first opening of the container will be recorded on the second line and will be the next number in sequence. All *SF 702s* must be labeled at the top of the form with the annotation of “ACREM.” (See attached *SF 702 for ACREM Containers* example.)

NOTE 2: The *SF 702* must be maintained in accordance with NARA requirements for receipts for classified matter (two years for Secret protected matter, and five years for Top Secret).

1. **Examine** the *SF 702* for the last recorded opening number (see column marked *Guard Check*) for the container to be opened.
2. **Dial** the lock **CONTINUOUSLY CLOCKWISE** (Right)  until a display is visible in the dial window. (Note: Continuously clockwise normally requires two-handed operation such that dialing must not be paused or stopped during this process—dialing may require up to 25 turns.) **STOP**. Read the two sets of two-each flashing numbers beginning with the set of numbers with the arrow pointing left; then the set of numbers with the arrow pointing right. (Example: Left Arrow reads 12; right arrow reads 34. The composite number is 1234.) There will always be four, and only four digits displayed. If you have, in error, dialed in the counterclockwise (left) direction first, **STOP**, wait for the display to disappear, then wait at least two more minutes before restarting this procedure with step 1.
3. **Compare** this number you are reading with the last recorded seal number (column marked *Guard Check*) on the *SF 702*. If these numbers do not match,

STOP, and summon your local security office. **DO NOT ATTEMPT TO DIAL THE COMBINATION**. If the numbers match, continue to step 4, below.

4. **Warning:** Do not execute this step unless the three steps above have been completed with matching XO audit numbers. Within 40 seconds of previous dial movement, reverse dialing directions and dial **COUNTERCLOCKWISE (Left)**  to begin the combination dialing process. If, during the first turn to the left a “lightning bolt” appears, **STOP**, and read the two digit number displayed with the lightning bolt. This number indicates that there have been “x” (≥ 3 but ≤ 99) unsuccessful opening attempts. Make a note of this number and report it as soon as possible to your local security office. The number of unsuccessful opening attempts will reset to “0” upon the first successful opening. Continue turning **COUNTERCLOCKWISE (Left)**  and dial the opening combination. Open the container.
5. Before proceeding, immediately *annotate* the *SF 702* with the date, time, your initials (ACREM Custodian/Alt), and the next in sequence opening number (column marked *Guard Check*) in the appropriate spaces. (Example: The last opening sequence number was 0967. You have verified, as above in steps 2 and 3, that the lock reads 0967. You now enter 0968 as the next opening sequence number.)

- **Closing Procedures**

1. **Close** the container. Turn the combination lock dial one full turn in the counterclockwise direction. Then turn the combination lock dial at least one full turn in the clockwise direction to ensure the lock is locked. (Note: if the dial stops and cannot be turned in the clockwise direction, the lock is not locked. Repeat this step.) Attempt to open the locking drawer and all other drawers with the lock in the locked mode.
2. **Annotate** the *SF 702* with the time and initials of the ACREM Custodian locking the container. A “double check” is required at the end of the work day. The person double checking the locked container does not need to be an ACREM custodian, but must ensure the container is locked by turning the combination lock dial at least one direction in the clockwise mode and attempting to open the container. The checking individual must annotate the SF-702 in the “checked by” column with the time and initials of the person performing the double check.

X-09 Abbreviated Procedures

(Note: Use only as a guide when detailed instructions are completely understood)

OPENING

1. Ensure there has been no lock dialing activity for two minutes after display has “blanked.”
2. Rotate lock dial **continuously clockwise** (right) to power up lock, and read the flashing “left arrow” / “right arrow” numbers displayed.
3. Compare this number with the last opening number (see column marked *Guard Check*) entered on the *SF 702*. If no match, **STOP**, and summon your local security office.
4. Dial counterclockwise (left). If a “lightning bolt” appears, stop, and note the number to be reported to your local security office at your next opportunity. Continue dialing counterclockwise (left) and proceed to open the lock.
5. Enter date, time, CREM Custodian initials, and next sequential opening number on the *SF 702*.

CLOSING

1. Close and lock the container, ensuring the dial has been turned one full turn in the counterclockwise direction.
2. Check to ensure lock is locked by rotating lock dial one full turn in the clockwise direction.
3. Check each drawer by attempting to open each drawer.
4. Annotate the *SF 702* with time and initials of a CREM custodian closing container.
5. At end of work day, obtain the assistance of another person to check the security condition of the container by performing steps 2 and 3, above. Annotate the *SF 702* in the “checked by” column. The person checking need not be a CREM custodian.

CONTRACTOR REQUIREMENTS DOCUMENT
DOE M 470.4-4, *Information Security*

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) contractors, including National Nuclear Security Administration contractors. Contractors must comply with the requirements listed in the CRD to the extent set forth in their contracts.

Regardless of the performer of the work, contractors with this CRD incorporated into their contracts are responsible for compliance with the requirements of the CRD. Affected contractors are also responsible for flowing down the requirements of the CRD to subcontracts at any tier to the extent necessary to ensure the contractors' compliance with the requirements. In so doing, contractors must not unnecessarily or imprudently flow down requirements to subcontractors. That is, contractors will ensure that they and their subcontractors comply with the requirements of the CRD and incur only those costs that would be incurred by a prudent person in the conduct of competitive business.

A violation of the provisions of this CRD relating to the safeguarding or security of Restricted Data 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. 228b.). The procedures for the assessment of civil penalties are set forth in Title 10, Code of Federal Regulations (CFR), Part 824, *Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations* (10 CFR part 824).

This CRD consists of the preceding Manual, DOE M 470.4-4, *Information Security*, with the exception of the following changes.

Information required to be submitted to the Office of Health, Safety and Security or its sub-elements must be submitted through the DOE Cognizant Security Authority.

The following paragraphs should be added or substituted for designated sub-sections.

Section A, Chapter II, 1. f. – Additional requirements

All contractors' procedures must be approved by the DOE cognizant security authority.

Section A, Chapter II, 9. b. – Additional paragraphs

Request for Release. Contractors must submit requests for release of U.S. classified information to foreign governments to the Departmental element with cognizance over the information. The contractor must assist the cognizant Departmental element with the development of the release justification (see Section A, Chapter II, paragraph 10.b.(4) of DOE M 470.4-4, *Information Security*). The Departmental element will then initiate review and approval actions within the Department.

Approval for Release. Contractors must not release any U.S. classified information to foreign governments without the prior written approval of DOE or in the case of RD/FRD, the written approval of DOE and the JAIEG. The JAIEG approval must be acquired through the NNSA Deputy Administrator for Defense Programs.

Section A, Chapter II, 9. b. (5) (a) – Replace existing text with paragraph below

Contractors must request that the Departmental element responsible for the classified information to be released to a foreign government initiate and coordinate all reviews necessary to effect the proposed classified information transfers.

Section A, Chapter II, 9. b. (5) (a) – Additional paragraph

Release of Classified. The contractor must not release any classified information to foreign governments without the express written approval of DOE.

Section A, Chapter II, 9. b. (6) (c) – Replace existing text with paragraph below

Contents. Contractors must follow the requirements made in information exchange agreements or as provided by DOE to ensure the security of the transferred documents, material, or information.

Section A, Chapter II, 9. b. (9) (a) – Replace existing text with paragraph below

Records on oral disclosures, made or contemplated, must be documented in memorandums transmitted to the Office of Health, Safety and Security.

Section A, Chapter II, 9. b. (9) (b) – Replace existing text with paragraph below

A record of the information being processed for release must be submitted through the cognizant Departmental elements to the Office of Health, Safety and Security.

SUBJECT: INFORMATION SECURITY

1. PURPOSE. To transmit revised pages to DOE M 470.4-4, *Information Security*, dated 6-29-07.
2. EXPLANATION OF CHANGES. To update the Manual's requirements for handling and protection of accountable classified removable electronic media (ACREM) to eliminate unnecessary resource burdens while maintaining protection and accountability for ACREM. Flexibility in how to implement certain security requirements is offered, but is bounded by required performance levels.
3. LOCATIONS OF CHANGES.

<u>Pages</u>	<u>Paragraphs</u>	<u>Pages</u>	<u>Paragraphs</u>
Cover	Chg 1 Office of Health, Safety and Security	II-16	3l(1)(b)5
		II-43	4b(2), 4b(4)
		II-44	4c(1), 4c(1)(a)-(b)
ii	5a, 5b	II-45	4c(2)
I-3	6e	II-47	4f(1)(a), 4f(1)(a) <u>1-2</u>
I-4	8a(2)(a), 8a(2)(a) <u>1</u> , footnote	II-48	4f(1)(a) <u>3</u>
I-5	8a(2)(c)	II-76	8c, 8c(5)
I-7	8b(4)(b), 8c	II-87	9d(2)
I-8	8c, 8c(1)(e)	II-88	Figure II-12
II-1	1d(1)-(3)	Section E	Contact information
II-2	1d(3)(a)-(c), Note		

BY ORDER OF THE SECRETARY OF ENERGY:



CLAY SELL
Deputy Secretary