DOE M 471.2-1C

This Manual cancels DOE M 471.2-1B, dated 1-6-99, except Chapter III paragraphs 1 and 2, and Chapter IV

Approved: 4-17-01
Sunset Review: 4-17-03
Expires: 4-17-05

CLASSIFIED MATTER PROTECTION AND CONTROL MANUAL

U.S. DEPARTMENT OF ENERGY
Office of Security and Emergency Operations
Office of Safeguards and Security

DISTRIBUTION:
All Departmental Elements

INITIATED BY:
Office of Security and Emergency Operations

CLASSIFIED MATTER PROTECTION AND CONTROL MANUAL

1. PURPOSE. This Manual supplements DOE O 471.2A, *Information Security Program*, and provides detailed requirements for the protection and control of classified matter.

2. CANCELLATION. This Manual cancels DOE M 471.2-1B, *Classified Matter Protection and Control Manual*, dated 1-6-99, except Chapter III paragraphs 1 and 2, and Chapter IV.

3. APPLICABILITY.

   a. General. This Manual applies to Department of Energy (DOE) elements, including the National Nuclear Security Administration, with access to classified matter.

   b. Contractors. This Manual applies to contractors with access to classified matter. All requirements contained in this directive apply to contractors and the entire directive is applicable to contractors. Procurement request originators must ensure that contracting officers are alerted of the applicable requirements in the Manual for each new procurement and for each affected existing contract.

4. USAGE. This Manual is composed of two chapters that provide detailed requirements for protection and control of classified matter. Chapter I provides a concise overview of protection and control planning considerations. Chapter II establishes control requirements for classified matter in use, marking of classified matter, accountability and control systems, reproduction, receipt and transmission, contract closeout or facility termination, and destruction.

5. DEVIATIONS. Deviations from the requirements in this Manual **must** be approved through procedures established in DOE O 470.1, *Safeguards and Security Program*.

6. REFERENCE. Terms used in this Manual are defined in DOE's "Safeguards and Security Glossary of Terms," dated 12-18-95.

7. ASSISTANCE. Questions concerning this Manual **should** be directed to the Classified Matter Protection and Control Program Manager, 301-903-2528.

8. IMPLEMENTATION. Most requirements in this directive are the same as those contained in DOE M 471.2-1B. Guidance formerly found in DOE G 471.2-1A, *Classified Matter Protection and Control*, has been incorporated into the Manual for ease of use. The reader will be able to distinguish between mandatory requirements and guidance because requirements are bolded using terms such as "**must**" and "**will**."

Guidance and recommendations are bolded using terms such as "**may**" and "**should.**" Implementation plans for any new requirements imposed by this Manual that cannot be implemented within 6 months of the effective date of this Manual or within existing resources **must** be developed by heads of field elements and submitted to the Lead Program Secretarial Office and the Office of Safeguards and Security, Office of Security and Emergency Operations.

SPENCER ABRAHAM
Secretary of Energy

CONTENTS

CONTENTS (continued)

TABLES

CHAPTER I

PROTECTION AND CONTROL PLANNING

1. SITE-SPECIFIC CHARACTERISTICS. Classified matter protection programs **must** be tailored to address specific site characteristics and requirements, current technology, ongoing programs, and operational needs, and to achieve acceptable protection levels that reduce inherent risks on a cost-effective basis.

2. THREAT. The "Design Basis Threat for the Department of Energy (DOE) Programs and Facilities (U)" **must** be used in conjunction with local threat guidance and vulnerability assessments for protection and control program planning.

3. PROTECTION STRATEGY.

   a. Strategies for the protection and control of classified matter **must** incorporate the applicable requirements established in this Manual. In addressing the threat to DOE's information assets, emphasis **must** be placed on security systems that will detect or deter unauthorized disclosure, modification, loss of availability, and unauthorized removal from a site or facility.

   b. Safeguards and security systems and critical systems elements **must** be performance tested to ascertain their effectiveness in providing countermeasures to address design basis threats.

4. PLANNING. Throughout this Manual there are references to the development of local procedures and other guidance documents that are necessary to the successful implementation of the provisions of this Manual. How the requirements set forth in DOE directives are accomplished will depend on circumstances unique to each facility. Local procedures will be necessary to ensure that these requirements are fulfilled in a consistent and uniform manner.

   a. Site Safeguards and Security Plans. The details of site protection measures for classified matter **must** be addressed in the Site Safeguards and Security Plan, as required by DOE O 470.1, *Safeguards and Security Program*.

   b. Security Plans. At locations where a Site Safeguards and Security Plan is not required due to the limited scope of safeguards and security interests, a security plan **must** be developed to describe the protection program in place.

5. TRAINING. Personnel whose responsibilities include the generation, handling, use, storage, reproduction, transmission (including hand-carry), and/or destruction of classified matter **must**

receive appropriate training to ensure such matter is not lost or compromised. Personnel with access authorizations whose job responsibilities do not meet the conditions specified above (e.g., personnel employed in maintenance, janitorial, food service, and other such activities) **must** be able to identify unprotected classified matter (e.g., classified cover sheets and classification markings) and know the appropriate reporting requirements.

a. Baseline Curriculum. Classified Matter Protection and Control (CMPC) training curriculums **must** be tailored to an individual's job responsibilities and **must** include the following subject areas: generation and marking, physical protection and storage, reproduction, accountability, transmission (including hand-carry), destruction, and emergency procedures, as it relates to the specific job responsibilities. All training **must** be developed in accordance with the requirements specified in Chapter II of DOE O 470.1, *Safeguards and Security Program*, and be tailored to the assigned duties and responsibilities of persons receiving training.

b. Frequency of Training. CMPC training **must** be provided before personnel have access to classified matter. All custodians/users and control station operators **must** receive refresher training at least once within 24 months of either the initial training or the date of the last refresher training. Personnel **must** be made aware of significant CMPC policy changes when they occur.

6. GRADED PROTECTION. By graded approach, DOE intends that, in the development and implementation of protection and control programs, the level of effort and magnitude of resources expended for the protection of a particular safeguards and security interest be commensurate with its importance or the impact of its loss, theft, compromise, and/or unauthorized use. Interests whose loss, theft, compromise, and/or unauthorized use would have serious impact on the national security and/or the health and safety of DOE and contractor employees, the public, the environment, or programs **must** be given the highest level of protection. For example, information that would assist an adversary in the development of a nuclear weapon or would assist an unauthorized person in bypassing use control systems, could have consequences so grave as to demand the highest attainable standard of security. Protection of other safeguards and security interests **are** graded accordingly. The results of asset valuation, threat analysis, 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.

Heads of Departmental elements **must** provide a rational, cost-effective, and enduring protection framework using risk management as the underlying basis for making security-related decisions. It **should** be recognized that certain risks will be accepted (i.e., it is impossible to eliminate the potential for, or consequences of, all malevolent events); however, an acceptable level of risk will be determined based on evaluation of a variety of facility-specific goals and

considerations. Protection-related plans **must** describe, justify, and document the graded protection provided the various safeguards and security interests.

7. MANAGEMENT FUNCTIONS. The CMPC managers' responsibilities **should** include *at least* the following:

   a. Planning. Writing CMPC plans and contributing to other plans [e.g., self-assessment, operations security (OPSEC), risk management, security, and operations]; writing local CMPC policies and procedures and ensuring that these procedures include all program elements (i.e., marking, accountability, transmission, reproduction, contract closeout/facility termination, and destruction); writing deviations to policy; and contributing to the budgeting process.

   b. Organizing. Participating in organizational structuring or restructuring, developing coordination interface protocols between CMPC and the other safeguards and security programs, and drafting job qualifications and descriptions.

   c. Staffing. Recruiting, orienting, developing, and training employees.

   d. Directing. Supervising and coordinating the daily activities of the CMPC program; troubleshooting and problem solving; participating in risk assessments, OPSEC assessments, and risk management; coordinating and integrating with related safeguards and security programs; communicating vertically and laterally; managing change; providing guidance and support to subordinates; and providing support and expert advice to clients and superiors.

   e. Controlling. Observing and reporting (e.g., security incidents involving classified information, inspection and survey results, self-assessment results, unauthorized disclosures, standard reports, etc.); developing standards and criteria for self-assessments; evaluating both the CMPC program and the program employees; conducting self-assessments; measuring results; and developing and completing corrective actions.

8. STORAGE—PROTECTING CONTAINER INFORMATION. The following storage requirements apply to classified matter. Items not covered in this section are provided in DOE M 5632.1C-1, *Manual for Protection and Control of Safeguards and Security Interests.*

   a. Protection of Security Containers and Combinations. The outside of the security container **must not** be marked to indicate that the contents are Top Secret, Secret, or Confidential. Security containers, vaults, and vault-type rooms used to protect safeguards and security interests **must** be kept locked when not under direct supervision of an authorized individual. Combinations **must** be classified and protected

at the classification level and category of the matter being stored within the container. Control measures **should** be implemented to ensure only the minimum number of personnel has access to the combination to the security container. Methods for protecting unauthorized access to combinations **should** be implemented and evaluated for effectiveness.

b. Part 1 of the SF 700 **must** be completed and affixed to the security container. On rooms or vaults, Part 1 of the SF 700 **must** be affixed to the inside of the door containing the combination lock. On security containers, it **must** be placed on the inside (back and front) of the locking drawer.

c. To ensure proper protection of the combination, Part 2a (the record of the combination) **must** be marked top and bottom with the highest level and category (if RD or FRD) of information contained within the security container. Part 2a is then inserted in the accompanying envelope (Part 2). The Part 2 envelope is then marked top and bottom, front and back, with the highest level and category (if RD or FRD) of information contained within the security container. Classifier information is not required to be identified on any part of the SF 700. Part 2 **must** then be forwarded to the central records for storage. If the combination protects information requiring additional authorized access (e.g., Sigma 14 and 15 or special access program information), the Part 2 cannot be sent to central records unless individuals at that location possess the same access requirements and need-to-know. In this situation an alternative storage location will be required.

d. Emergency notification personnel or repository custodians **must** be listed on the SF 700. A record of all persons who know the combination also **must** be maintained. This record **should** be maintained with both Part 1 and Part 2 of the SF 700. An additional record is not required if the individuals are listed on the SF 700 and are the only persons who know the combination.

e. Changing Combinations. Combinations **must** be changed by an appropriately cleared and authorized individual, as soon as practicable upon:

(1) initial receipt of a GSA-approved security container or lock;

(2) one of the following events occurring to an individual who knows the combination:

(a) reassignment, transfer, or termination of employment;

(b) downgrading of DOE access authorization to a level lower than the level of classified matter stored; or

(c) administrative termination or suspension of DOE access authorization;

(3) following maintenance by an uncleared locksmith or safe technician;

(4) compromise or suspected compromise of a security container or its combination, or discovery of a security container containing classified matter which is unlocked and unattended.

(5) preparation for turn-in of the container. The combination **must** be set to factory standard 50-25-50 prior to turn-in of the container.

NOTE: Combinations used to protect communications security material will be changed biennially, at a minimum, or in accordance with the requirements contained in DOE M 200.1-1, *Telecommunications Security Manual*.

f. 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 numbers that are easily associated with the person(s) selecting the combination (e.g., birth dates, anniversaries, social security numbers, or telephone extensions).

g. Security Repository Information. Applicable requirements concerning security repositories are provided below.

(1) Security Container Information. An SF 700 **must** be completed for all security containers, rooms, vaults, and other approved locations for the storage of classified matter.

(2) Security Container Check Sheets. An integral part of the security check system **must** be ensuring that classified matter has been properly stored and that security containers, vaults, or vault-type rooms have been secured. SF 702, Security Container Checklist, **must** be used to record the end-of-day security checks.

(a) The SF 702 **must** be used to record the names and times of the persons who have opened, closed, or checked a particular container, room, or vault holding classified information.

(b) The SF 702 **must** be used in all situations requiring the use of a security container check sheet and **must** be affixed to the container or entrance to a room or vault. A sole custodian of a security container it is not required to record each opening and closing of the container throughout

the day. In such cases, the appropriate information **should** 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 **should** be recorded indicating the final closing of the container for that day. If two or more persons share the container, each opening and closing **must** be duly recorded.

(c) Checks at the end of the day **should** be performed by someone other than the person closing the container. Facilities **should** develop procedures to ensure security containers are secured and end of day checks are performed by an individual other than the one that secured the container.

(3) Activity Security Checklist. SF 701, Activity Security Checklist, 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. The checklist identifies such activities as checking security containers, desks, and wastebaskets for classified matter and ensuring that windows and doors are locked, ribbons for classified typewriters and automated data processing equipment have been secured, and security alarms have been activated. Use of the SF 701 is optional, except in situations requiring detailed end-of-day security inspections, when its use is mandatory.

(4) Records. Completed SF 701s and SF 702s **must** be maintained according to General Records Schedule 18.

CHAPTER II

CLASSIFIED MATTER PROTECTION AND CONTROL

1. GENERAL. The protection requirements described in this chapter are consistent with the requirements set forth in the National Industrial Security Program Operating Manual of January 1995 and its supplement of February 1995.

   a. Classification level and category **must** be used in determining the degree of protection and control required for classified matter.

   b. Access to classified matter **must** be limited to persons who possess appropriate access authorization and who require such access (need-to-know) in the performance of official duties; access is not obtained by position only. Controls **must** be established to detect and deter unauthorized access to classified matter.

   c. The originator of matter that is prepared in a subject area that is or **may** be classified **must** ensure the matter is reviewed for classification by a derivative classifier. While the matter is pending classification review, it **must** be protected at the highest potential classification level and category. Should any question exist regarding the classification of any draft documents or working papers, the originator is responsible for obtaining a classification review.

   d. When information is prepared on classified information systems, hard-copy output (which includes paper, fiche, film, and other media) must be marked to the accreditation level of the information system unless an appropriate classification review has been conducted or the information has been generated by a tested program verified to produce consistent results and approved by the Designated Accrediting Authority. An appropriate sensitivity and classification review must be performed on human-readable output before the output is released outside the system boundary to determine whether it is accurately marked with the appropriate classification and applicable associated security markings.

   e. When the classification of matter cannot be determined and information must be sent outside the office of origin to an appropriate official for a classification review and determination, it must be marked "DRAFT - Not Reviewed for Classification." In order 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.

f. In medical emergency situations, classified information **may** be provided to the attending physician when such information is essential for the treatment of the patient. In these situations, a report of unauthorized disclosure **must** be submitted in accordance with DOE requirements.

g. Custodians and authorized users of classified matter are responsible for the protection and control of such matter. In accordance with the memorandum issued by the Secretary of Energy to all DOE and contractor employees, dated 6-17-99, the responsibility for protecting classified and sensitive information and nuclear and other sensitive material lies with the individual. This memorandum established a policy of "zero tolerance" for violations of security requirements that place nuclear or other sensitive material or information at risk or result in their compromise. Employees who fail to comply with established security requirements will be subject to prompt administrative actions, which may include a written reprimand, mandatory remedial training, and access authorization eligibility review.

All DOE and DOE contractor employees **should** be provided information regarding the Secretarial Policy Statement on "zero tolerance" to ensure they understand their personal responsibilities and the consequences for failing to comply with the policy. Methods for providing this information to all DOE and DOE contractor employees **may** include electronic distribution, briefings, awareness bulletins, etc.

h. Buildings and rooms containing classified matter **must** be afforded security measures necessary to prevent unauthorized persons from gaining access, including unauthorized visual access, to classified information.

i. Though most of the requirements in this chapter apply to Foreign Government Information (FGI), a separate paragraph contains requirements specific to this information. (See paragraph 10.)

j. Classified matter, including "extra copies," is the property of the U.S. Government and **must not** be removed from the Government's control by any departing, including terminated, DOE or contractor employee. The Facility Security Officer **must** establish control measures for the retention of all classified Departmental records that **may** be in the possession of departing employees.

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 a need-to-know, except as specified below. When defense-in-depth exists, local DOE safeguards and security authorities **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, Protected Area, Material Access Area, or Exclusion Area. 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 not** be similar to 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 will not be used as a routine method of protection. This practice **must not** be used on Sensitive Compartmented Information facilities, vaults or vault-type rooms.

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 3a(1), which **must** be followed.

a. General.

(1) Requirement. Classified matter, regardless of date or agency of origin, **must** be marked to indicate at least the classification level and category [if Restricted Data (RD) or Formerly Restricted Data (FRD)]. Documents dated after 4-1-96, **must** be marked in accordance with directives in place at the time of origin or in accordance with current directives.

(a) If there is a question about the classification level or category of a document generated before the publication of DOE M 471.2-1, the document **should** be reviewed by a derivative classifier and re-marked (if necessary) to clearly indicate the level and category to ensure proper protection.

(b) Classified documents that were created after implementation of DOE M 471.2-1 and lack markings indicating declassification on a date or event, classification authority, or classifier's name, **should** be reviewed by a derivative classifier and re-marked if necessary.

(c) Documents created prior to 4-1-96, need only contain classification level and category (if RD or FRD), to ensure proper protection. With the implementation of DOE M 471.2-1, documents created *after* 4-1-96, and *prior* to the implementation of DOE M 471.2-1A (6-month implementation date of 7-9-98) need to meet the requirements of DOE M 471.2-1.

(d) Before using or distributing a document marked with the following obsolete markings, a derivative classifier **must** determine the classification status and mark the document accordingly. 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 prior to 12-15-53, identifying a security level less sensitive than Confidential. This marking is still used by some foreign governments and international organizations.

2 Official Use Only. The Atomic Energy Commission used this term between 7-18-49 and 10-22-51 as an equivalent to the term Restricted. This marking is now used to identify unclassified information that maybe exempt from disclosure under the Freedom of Information Act.

(e) When possible, avoid returning transmitted classified documents. If a document is improperly marked, discuss the problems by telephone with the transmitting office, and attempt to resolve marking issues. This technique is much faster, more efficient, and ensures continued control of the classified information. Sometimes it is critical to return the document, such as when it does not have classifier information. Issues like no classification level stamp on the back of the document would be considered minor and could be corrected at the receiving facility.

(2) Markings. The following elements are common to all classified documents: classification level, classification category (if RD or FRD), caveats (special markings), classifier information, originator identification, classification of titles, unique identification numbers (accountable only), and portion marking (if NSI). The DOE Marking Handbook (available at www.explorer.doe.gov) provides guidance and examples for the marking of classified documents. Types of documents not addressed in the Handbook will be provided in this Manual. Any deviation from these markings will be specifically stated. The originator is responsible for ensuring each document is marked with the markings identified in this chapter. DOE M 475.1-1, *Identifying Classified Information*, requires that the derivative classifier ensure the classification level, category (if RD or FRD), and classifier information are included on each document.

(3) Unique Identification Numbers. Classified matter required to be in accountability, as defined in paragraph 4, Control Systems and Accountability, **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 (preferably in the upper right corner) and on the top/front

of nonpaper documents. The first page of a document is the first sheet of paper; either the cover page, title page, or first page of text.

(4) Commingling Documents. Top Secret, Secret, Confidential, and Unclassified documents **may** be commingled. For example, Top Secret, Confidential, and Unclassified documents **may** be stored in the same file folder. Need-to-know considerations, however, might make it necessary to segregate documents. For example, it might be necessary to avoid photographing Top Secret documents onto the same reel or microfiche as Secret or Confidential documents. Good business practice suggests marking commingled unclassified documents as Unclassified when stored/filed with classified documents.

Electronic removable media that contains Sigmas 1, 2, 14, or 15 or a combination of nuclear weapons design/test data or Top Secret or Special Access Program matter **must** be separated from and not commingled with other classified information/media. This may be accomplished with the use of file folders or similar methods.

(5) Material. Material (i.e., parts, hardware, etc.) marking is discussed in paragraphs c(5) and d(3) below and in paragraph 11 of this chapter.

b. Originator Identification and Date. When leaving the facility, classified documents **must** be marked on the first page to show the name and 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. This can be accomplished by printing the first page of the classified document on company letterhead, if the letterhead identifies the complete name and mailing address of the originating organization, or by adding the name and mailing address to the first page of the document. The first page of a document is the first sheet of paper, either the cover page, title page, or first page of text.

All classified documents **must** identify the date of preparation on the first page.

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), on the title page (if any), on the first page, and on the outside of the back cover or last page.

(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) These document markings **must** be clearly distinguishable from the informational text. At least one blank line **should** be placed between the level and the text. The level markings can be of a larger font, different color, or both to distinguish this marking from the text. The key is to ensure a clear separation between the text and the level marking.

(5) Classified material **must** have the classification level stamped, printed, etched, written, engraved, painted, or affixed 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) Use of a back cover sheet is an acceptable practice. If not using a back cover sheet, good business practice suggests placing a blank sheet at the end of classified documents that contain information on the back of the last page. If a blank sheet is used, it **must** be marked in accordance with paragraph 3c(2). If no text appears on the back of the last page, it **should** be marked with the overall classification level of the document.

(7) 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 Category. The three classification categories are RD, FRD, and NSI. Classified documents containing only NSI need *not* be marked with the NSI category marking.

(1) The overall category (if RD or FRD) of a document **must** be marked on the first page of the document. This marking **should** appear on the lower left corner.

RESTRICTED DATA
This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal Sanctions.

FORMERLY RESTRICTED DATA
Unauthorized disclosure subject to Administrative and Criminal Sanctions. Handle as Restricted Data in Foreign Dissemination, 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 category of that page. If this is not feasible, the overall category of the document (if RD or FRD) **may** be applied to every page. For interior pages, the symbols "RD" for Restricted Data and "FRD" for Formerly Restricted Data **may** be used. These markings **must** be clearly distinguishable from the informational text.

(3) Classified material (if RD or FRD) **must** have the classification category stamped, printed, etched, written, engraved, painted, or affixed 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) If significant cost and extensive reprogramming of automated information systems are required to implement this requirement, facilities **may** delay implementation until 1-9-03, as long as documents generated from the automated information system remain on site and have a limited life expectancy.

(5) RD or FRD documents generated prior to the implementation of DOE M 471.2-1A will not be required to be re-marked to indicate the category on each page containing RD or FRD information.

e. Mixed Levels and Categories. DOE policy states that matter will be classified and marked at the highest level and category of the information contained in it. When classified matter contains a mix of levels and categories that causes it to be marked at an overall level and category higher than the protection level required for the individual portions, a matrix **may** be used in addition to other required markings. A marking matrix **may be** necessary to allow access for "L" cleared employees without compromising security. The marking matrix should be placed 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. 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. If a matrix is used, the following marking matrix, in addition to other required markings, **must** be placed on the first page of text. The marking **should** appear on the lower right corner.

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 to a letter, 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, such as "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.

Unclassified components marked as containing only unclassified information can be removed by the recipient without having to re-mark the unclassified or classified portion of the document. When unclassified components are removed from a classified document, the recipient is not required to have the document reviewed to ensure the classification of the document is unchanged. If the classification of a classified document will change when an unclassified component is removed, the component **must** be treated as part of the classified document.

Documents transmitted with a letter of transmittal are discussed in paragraph 3s, 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., Official Use Only (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 4-1-97, **must** be marked to show the classification level or be identified as unclassified. In marking portions, the symbols (TS) for Top Secret, (S) for Secret, (C) for Confidential, (U) for Unclassified, (UCNI) for Unclassified Controlled Nuclear Information, and (OUO) for Official Use Only **must** be used. 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 4-1-97, **must** be portion marked.

(3) Documents containing RD or FRD are not required to be portion marked.

(4) Portion markings **must** include caveats (as applicable).

(5) Portions of U.S. documents containing FGI **must** be marked to reflect the foreign country of origin as well as the 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 that it does not want to be identified. 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 (RD or FRD) or an appropriate international agreement (NSI) specifically allowing the sharing of these categories and levels of classified information, the document may not be returned to the originating government or international organization of governments.

(6) 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)].

i. Subjects and Titles. Except for extraordinary circumstances, unclassified subjects and titles **must** be used for classified documents. If subjects or titles are classified, they **must** be marked with the appropriate classification level, category (if RD or FRD), and any applicable caveats. The classification symbols (e.g., U, CRD, S/ORCON) **must** be placed immediately after the title or subject.

(1) Markings. The following are examples of the markings authorized for use with subjects and titles and when portion marking:

(a) Unclassified: (U)

(b) Official Use Only: (OUO)

(c) Unclassified Controlled Nuclear Information: (UCNI)

(d) Confidential National Security Information: (C)

(e) Confidential Formerly Restricted Data: (CFRD)

(f) Confidential Restricted Data: (CRD)

(g) Secret National Security Information: (S)

(h) Secret Formerly Restricted Data: (SFRD)

(i) Secret Restricted Data: (SRD)

(j) Top Secret National Security Information: (TS)

(k) Top Secret Restricted Data: (TSRD)

(l) Top Secret Formerly Restricted Data: (TSFRD)

(2) Caveats. If a caveat, such as ORCON (Originator Controlled), 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).

(3) Classification. Unclassified subjects or titles **must** be used, except for extraordinary circumstances, because they are used on mail logs, document receipts, and other tracking or accountability records, most of which are entered into unclassified data bases.

(4) Unmarked Titles. When classified documents with unmarked titles or subjects become active (i.e., sent outside the office of origin or holder, or removed from storage), the title or subject **must** be reviewed by a derivative classifier and marked appropriately.

j. Authorized Classifiers. DOE has two types of authorized classifiers: original and derivative. Original classifiers **must** be Federal employees authorized to make original classification decisions on NSI information. Derivative classifiers **may** be either Federal or contractor employees who are designated to classify any or all levels and categories of derivatively classified documents, including the various

caveats. For additional information regarding classification authorities please refer to DOE M 475.1-1.

k. Classifier Markings. The following information describes the classifier marking requirements and provides an example of each marking and instructions for completing each line. For NSI documents, classifier markings **should** be placed on the lower left corner of the first page of the document. For RD and FRD documents, the classifier markings **should** be placed on the lower right corner of the first page of the document. The first page of a document is the first sheet of paper, either the cover page, title page, or first page of text. Classifier markings **must** be applied as follows:

(1) Original Classification (NSI only).

(a) Classification authority (i.e., "Classified By").

1 Typed or printed name or personal identifier of the original classifier.

2 Position title of the original classifier.

This line does not require a signature, but good business practice suggests that local procedures **should** require a signature. The term "signer" can be used to complete this line if the signer of the document also is the classifier of the document.

(b) NSI classification category (i.e., "Reason"). Information not contained in a classification guide or source document cannot be originally classified as NSI unless it concerns one of the seven NSI classification categories listed in Executive Order 12958, section 1.5. The original classifier **must** identify the reason for the decision, and enter "1.5" (the section of Executive Order 12958) and the classification category(ies) or corresponding letter on the "Reason" line, [e.g., 1.5(a)]. The seven NSI classification categories are as follows (these categories are *not* the same as RD and FRD):

1 Military plans, weapons systems, or operations.

2 FGI.

3 Intelligence activities (including special activities), intelligence sources or methods, or cryptology.

4 Foreign relations or foreign activities of the United States, including confidential sources.

5 Scientific, technological, or economic matters relating to the national security.

6 U.S. Government programs for safeguarding nuclear materials or facilities.

7 Vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security.

(c) Duration of classification (i.e., "Declassify On").

1 Date. A specific date 10 years or less from the date of the original decision.

2 Event. A specific event occurring in less than 10 years.

3 Exempt from declassification. Document is exempt from declassification at 10 years and identified by an exemption category (e.g., X1 through X8).

If a document is exempt from automatic declassification at 10 years, complete the "Declassify On" line with the letter "X" followed by either the exemption number or a brief recitation of the exemption. The eight exemptions listed in Executive Order 12958 are summarized as follows:

X1 Reveal an intelligence source, method, or activity, or a crypto logic system or activity.

X2 Reveal information that would assist in the development or use of weapons of mass destruction.

X3 Reveal information that would impair the development or use of technology within a U.S. weapons system.

X4 Reveal U.S. military plans or national security emergency preparedness plans.

X5 Reveal FGI.

X6 Damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than 10 years.

X7 Impair the ability of responsible U.S. Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized.

X8 Violate a statute, treaty, or international agreement.

4 Extension of classification. Classification of the information **may** be extended for successive periods not to exceed 10 years at a time. The "Declassify On" line **must** be revised to include the date of the extension action, the new declassification date, and the identity of the person authorizing the extension.

5 Reclassification. Information **may** be reclassified for successive periods not to exceed 10 years at a time. The "Declassify On" line **must** be revised to include the date of the reclassification, the new declassification date, and the person authorizing the reclassification.

(d) Example original classifier marking.

Classified By: *(Name/Personal Identifier and Position Title)*
Reason: *(NSI Classification Category)*
Declassify On: *(Date, Event, or Exemption Category)*

(2) Derivatively Classified NSI.

(a) Classification authority (i.e., "Classified By").

1 Typed or printed name or personal identifier of the derivative classifier.

2 Position title of the derivative classifier.

This line does not require a signature, but good business practice suggests that local procedures should require a signature. The term "signer" can be used to complete this line if the signer of the document also is the classifier of the document.

(b) Designation of the guidance or source document(s) and date of such documents. Insert the name of the classification guide or source document and the date of the guide or source document on the "Derived From" line. The date used for the guide **must** reflect the most recent change notice only if the change notice actually changes the date of the guide. If the classification of a document was derived from more than one source, the words "Multiple Sources" **may** be used to complete the "Derived From" line. When multiple sources are used, the identification of each source **must** be maintained with the record copy of the document.

(c) Duration of classification (i.e., "Declassify On").

1 Date. A specific date 10 years or less from the date of the document, as specified by the guidance or source document(s).

2 Event. A specific event occurring less than 10 years from the date of the document as specified by the guidance or source document(s).

3 Exempt from declassification. Document is exempt from declassification at 10 years and identified by an exemption category (e.g., X1 through X8) as specified by the guidance or source document(s). [See paragraph 3k(1)(c)3.]

4 Extension of classification. Classification of the document **may** be extended for successive periods not to exceed 10 years at a time. The "Declassify On" line **must** be revised to include the date of the extension action, the new declassification date, and the person authorizing the extension.

5 Reclassification. As appropriate, a document **may** be reclassified. The "Declassify On" line **must** be revised to include the date of the reclassification, the new declassification date, and the person authorizing the reclassification.

(d) 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. An example of the use of the OADR marking on a new document is as follows:

Classified By: *(Name/Personal Identifier and Position Title)*
Derived From: *(Title and Date of Source)*
Declassify On: *(Source Marked "OADR")*

(e) Example NSI derivative classifier marking.

Classified By: *(Name/Personal Identifier and Position Title)*
Derived From: *(Guide/Source Document and Date)*
Declassify On: *(Date, Event, or Exemption Category)*

(3) RD and FRD.

(a) Classification authority (i.e., "Classified By").

1 Typed or printed name or personal identifier of the derivative classifier.

2 Position title of the derivative classifier.

This line does not require a signature, but good business practice suggests that local procedures **should** require a signature. The term "signer" can be used to complete this line if the signer of the document also is the classifier of the document.

(b) Designation of the guide or source document and date of such document(s) (i.e., "Derived From").

1 Insert the name of the classification guide or source document and the date of the guide or source document on the "Derived From" line. The date used for the guide **must** reflect the most recent change notice, if this change notice changes the date of the guide.

2 If the classification of a document was derived from more than one source, the words "Multiple Sources" **may** be used to complete the "Derived From" line. When multiple sources are used, the identification of each source **must** be maintained with the record copy of the document.

(c) Example RD and FRD classifier marking.

Classified By: *(Name/Personal Identifier and Position Title)*
Derived From: *(Guide/Source Document and Date)*

l. Caveats. Classified matter **must** be marked with caveats, such as those indicated below, when required by DOE directive or national policy. Caveat markings are placed on documents either to identify special handling or dissemination requirements or to assist in describing the type of information and who distributed or originated the information. Caveat markings **should** be placed above the category marking or on the lower left corner of the first page, either cover page, title page, or first page of text. If the caveat has an abbreviated form, the abbreviation **may** be used in place of the full-text caveat marking.

(1) 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.

This notation applies to documents whose further dissemination within the receiving contractor facility is restricted to persons authorized by the addressee. Dissemination outside the facility is prohibited without the approval of the contracting activity.

(b) REPRODUCTION REQUIRES APPROVAL OF ORIGINATOR.

This notation applies to documents that **must** not be reproduced without the specific, written approval of the originator.

(2) FGI. Marking, protection, and control requirements for FGI are contained in paragraph 10.

(3) NATO Information.

(a) NATO Classified. NATO has four levels of classified information: COSMIC Top Secret (CTS), NATO Secret (NS), NATO Confidential (NC), and NATO Restricted (NR). When "NATO" or "COSMIC" precedes a classification, the information is the property of NATO. NATO classified information **must** be safeguarded in

compliance with United States Security Authority for NATO Instructions I-69 and I-70.

(b) NATO Restricted. NATO information and material which requires security protection, but less than that required for Confidential.

(c) ATOMAL. The ATOMAL category is either U.S. RD or FRD or United Kingdom Atomic Information that has been officially released to NATO. ATOMAL information is classified either COSMIC Top Secret ATOMAL (CTSA), NATO Secret ATOMAL (NSA), or NATO Confidential ATOMAL (NCA), depending on the damage that would result from unauthorized disclosure.

(4) Director of Central Intelligence Information. The following are markings authorized for use only for Intelligence Information: No Foreign Dissemination (NOFORN), Originator Controlled (ORCON), Proprietary Information (PROPIN), and Authorized for Release to Country (REL TO).

(a) NOFORN. This marking indicates that 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.

(b) ORCON. This marking indicates that the document bearing the marking is controlled by the originator. Reproduction, extraction of information, or redistribution of such documents requires the permission of the originator. This marking **must** be used only on classified 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 will be reasonably protected by use of its classification markings or by use of 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 to the receipt of ORCON by a non-intelligence component, as with any classified information, written assurance must be provided to the Office of Intelligence that the recipient will observe the provisions of the Director of Central Intelligence Directive.

(c) PROPIN. This marking indicates that 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 and provider of the proprietary information. This precludes dissemination to contractors irrespective of their status to or within the Government, without the above consent.

(d) 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 a specified foreign country(ies) or international organization(s).

(e) The intelligence community no longer uses the following markings: No Dissemination to Contractors (NOCONTRACT) and Warning Notice—Intelligence Sources and Methods (WNINTEL).

(5) Weapon Data. The following markings are associated with atomic weapons or nuclear explosive devices.

(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 defined as Sigma 14 and 15 information.

(b) Critical Nuclear Weapons Design Information (CNWDI). This is a Department of Defense marking designating Top Secret or Secret Restricted Data that reveals the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munitions, or test device. For more details, refer to DOE 5610.2, *Control of Weapon Data*.

(6) 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 statute. Questions regarding NNPI **must** be directed to the Assistant Administrator for Naval Reactors.

(a) Access. Access to NNPI **must** be granted only to U.S. citizens who have a need-to-know.

(b) Marking. 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 the NavSea." (This marking should be placed on the front 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.

(7) SPECAT. This is a Special Category (SPECAT) program controlled by the Department of Defense which generally operates at the Secret level. It is not a Special Access Program nor is it a code word. SPECAT programs utilize Focal Point Control Officers (FPCO) to control the dissemination and handling of NSI contained within the program. There are a number of SPECAT programs in DOE. NNSA is the DOE Primary FPCO for SPECAT and should be contacted for additional information regarding the program.

m. Re-marking Upgraded, Downgraded, and Declassified Matter. Upon receiving an official upgrade, downgrade, or declassification notice, the initial classification level markings **must** be stricken and replaced with the new classification level markings. The authority for and date of the upgrading, downgrading, or declassification notice **must** be entered on the first page of the document. The originating agency **must** notify all known holders of the document.

(1) General. Refer all upgrading, downgrading, and declassifying issues to the declassification office. For details, see DOE M 475.1-1, *Identifying Classified Information*, Chapter VI.

(2) Record Retention. Good business practice suggests that the copy of the change notice **should** be retained with the record copy of the document until the document is destroyed. The control station also **should** maintain a copy.

The original change notice is considered record material and must be retained in accordance with Schedule 18 of the General Records Schedules.

(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 notice from the proper authority. The originating agency **must** notify all known holders, with the proper access authorization, of the document that 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 following:

(a) the date the classified document was upgraded and

(b) the authority for upgrading the document (e.g., a memorandum, an Office of Scientific and Technical Information notice, a classification guide, or a guide topic).

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

CLASSIFICATION RETAINED DOE NSI DECLASSIFICATION REVIEW EXECUTIVE ORDER 12958 EXEMPTION/RETENTION BY CG-HR-1 TOPIC(S): _____ BY (NAME) DOE/SO-223	This stamp would be used when reviewing a DOE or other agency NSI classified document that contains DOE classified information exempt from automatic declassification.
CLASSIFICATION CANCELED DOE NSI DECLASSIFICATION REVIEW EXECUTIVE ORDER 12958 BY (NAME) DOE/SO-223	This stamp would be used when reviewing a DOE NSI classified document that no longer contains DOE or other agency classified information.
CONTAINS NO DOE CLASSIFIED INFO DOE NSI DECLASSIFICATION REVIEW EXECUTIVE ORDER 12958 BY (NAME) DOE/SO-223	This stamp would be used when reviewing an other agency document that the review confirmed contained no DOE classified information.
CONTAINS NO DOE CLASSIFIED INFO COORDINATE WITH:_____ DOE NSI DECLASSIFICATION REVIEW EXECUTIVE ORDER 12958 BY (NAME) DOE/SO-223	This stamp would be used when reviewing a DOE NSI classified document that no longer contains DOE classified information but may contain other agency classified information. The agency's name would be filled in.
CONFIRMED TO BE UNCLASSIFIED DOE NSI DECLASSIFICATION REVIEW EXECUTIVE ORDER 12958 BY (NAME) DOE/SO-223	This stamp would be used when reviewing a DOE purportedly unclassified document that is confirmed to contain no currently classified information.
WITH ATTACHMENTS/ENCL	This 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.
WITHOUT ATTACHMENTS/ENCL	This 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 that the review did not apply to the attachments/enclosures.
THIS PAGE ONLY	This would be used to indicate that the review was only conducted of a single page; e.g., one page separated from a multipage document.

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. Downgrading takes two authorities (e.g., a derivative classifier and a derivative declassifier). The custodian of a document or material **may** downgrade its classification markings upon receipt of notice from the proper authority. Upon receipt of the authorization to downgrade a classified document, the first page of the document **must** be marked to show the following:

(a) the date the classified document was downgraded and

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

Example of downgrade marking:

Classification Downgraded: *(Insert Date Document was Downgraded)*
Downgrade Authority: *(Authority for Change in Classification)*

(6) Declassifying. A derivative declassifier **may** derivatively declassify only documents or material originated in those organizations and subject areas for which he/she has been delegated such authority and is governed by other limitations specified in the written designation. A derivative declassifier **must** base his/her determinations on classification guidance pertaining to the specific subject areas described in the declassifier's designation of authority. Declassifying takes two authorities (e.g., a derivative classifier and a derivative declassifier). The classification markings **must** be crossed out, marked as unclassified, and the following information applied to the first page of the document.

(a) The name(s)/personal identifier(s) and position title(s) of individual(s) declassifying the document are identified on the "Declassified By" line.

(b) The designation of the guidance or source document(s) used as the basis for the declassification determination and the date of such document(s) are identified on the "Derived From" line.

(c) The date of declassification is identified on the "Declassified On" line.

(d) Example of declassification marking:

Declassified By: *(Name/Personal Identifier and Position Title)*
Derived From: *(Designation of guidance or source document and date of such document)*
Declassified On: *(Date of Declassification)*

n. Re-marking Automatically Declassified Matter. Matter marked for automatic declassification **may** be declassified and re-marked 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.

o. Classified Matter Not Automatically Declassified. The following types of classified matter are not automatically declassified: matter containing RD or FRD, DOE matter marked as containing NSI that does not specify a date or event for declassification, and matter marked as exempt from automatic 10-year declassification.

p. Classified Matter Marked for Declassification. Classified matter marked with a specific date or event for declassification is declassified after the date or event has passed. Once declassified, anyone **may** remove or obliterate the classification markings from all pages. The first page of the document **must** be marked "Unclassified" on the top and bottom.

q. 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 standard (8.5 × 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 office to be operationally necessary. The unique identification number, if required, **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) Electronic Mail (E-Mail) Messages.

(a) Classified e-mail messages can be transmitted only on systems approved for classified transmissions and in accordance with the system security plan. The sender is responsible for indicating on the first line of text the overall classification level, category (if RD or FRD), and applicable caveats, of the entire message (to include attachments). This information must be clearly distinguishable from the body of the message. The last line of text must contain the overall classification level and category (if RD or FRD). All other required classification markings for final documents [e.g., classifier information, category admonishment, portion marking (NSI only), subject/title markings, unique identification number (if accountable)] must be provided in the message text.

(b) Classified e-mail messages containing classified attachments must be marked as identified above. The classified attachment also must contain the classification markings required for a final document.

(c) Unclassified e-mail messages containing classified attachments must be marked to indicate the overall classification level, category (if RD or FRD), and applicable caveats of the attached document. The classified attachment must contain the classification markings required for a final document.

(d) If the classified e-mail message is a working paper or draft, then the e-mail message will be marked as such and in accordance with Chapter II paragraph q(3) of this Manual. If the e-mail message is transmitted outside the originator's activity or office it must be marked as a final document. Facility personnel should define "originator's activity/office" in their local implementing procedures.

(e) The recipient is responsible for applying the appropriate classification markings [e.g., ensuring level and category (if RD or FRD) is placed on the top and bottom on every page], if the message is printed in hard copy at the receiving location.

(f) The first line of an unclassified e-mail message sent on a classified e-mail system must indicate that the message is unclassified. If the e-

mail contains other sensitive unclassified information it should retain its unclassified marking.

(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 1325.7A, Telecommunication Message, may be used as the first page of the facsimile. This form or a locally developed form can be marked either as an unclassified letter of transmittal or as the first page of the classified document. See Figure II-1.

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 all previous recipients receive a correctly marked version with instructions to destroy all previous draft copies.

(5) Microforms.

(a) Microforms contain images or text in sizes too small to be read by the unaided eye. Markings **must** consider the media involved but **must** be readable by the unaided eye.

(b) All required markings **must** be on the individual documents contained on the microforms.

(c) 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).

(d) Good business practice suggests that all unclassified documents placed on microforms be marked Unclassified, which ensures that all documents on a classified microform are specifically identified as being either unclassified or classified.

(e) Microforms created prior to 7-15-94, need *not* be redone if all documents contained in them are not marked as independent documents.

DOE F 1325.7A (3-83)
SACNET USER'S GUIDE
Previous Editions are Obsolete.

1. INSERT ABOVE, CLASSIFICATION LEVEL, UNCLASSIFIED, OR OFFICIAL USE ONLY

2. MESSAGE CONTAINS WEAPON DATA?
("X" appropriate box. Message center will not transmit message unless box is marked.)
G YES **G** NO

U.S. DEPARTMENT OF ENERGY
TELECOMMUNICATIONS MESSAGE (DATA)
(See reverse side for instructions.)

3. USE WHEN REQUIRED
THIS DOCUMENT
CONSISTS OF _____ PAGES
NO. ____ OF ____ COPIES, SERIES ____

4. PRECEDENCE DESIGNATION *("X" appropriate box):*

FOR NORMAL USE	EMERGENCY USE ONLY
ACTION: **G** Routine **G** Priority	**G** Immediate **G** FLASH
INFO: **G** (6 Hrs.) **G** (3 Hrs.)	**G** (30 Mins.) **G** (ASAP)

5. TYPE OF MESSAGE
("X" appropriate box)
G *Single Address*
G *Multiple Address*
G *Title Address*
G *Book Message*

FOR COMMUNICATION CENTER USE
MESSAGE IDENTIFICATION
NR: DTG: Z:

6. FROM

7. OFFICIAL BUSINESS (TIME)
(Signature of authorizing official)
A.M. P.M.

8. DATE

9. TO

COMMUNICATION CENTER ROUTING

9a. SPECIAL HANDLING INSTRUCTIONS:

69 Elite 69 Pica

9b. DATA INPUT DESCRIPTION:

Mag. Tape ( ) 7 Track ( ) 200 BPI ( ) 556 BPI ( )
Cards ( ) 9 Track ( ) 800 BPI ( ) 1600 BPI ( )
Data Location: Attached ( ) Library ( ) Other_____
Job Name: _____

Record Lengths: Variable ( ) Fixed ( ) Reel No. _____
Max. Physical Record Size _____ char. Labeled MT ( )
Min. Physical Record Size _____ char. Unlabeled MT ( )
Single File ( ) Multi-File ( ) Logical Record Count ( ) Block Factor ( )
Formatted Print File ( ) Unformatted Print File ( )

9c. DATA OUTPUT AT DESTINATION:

Magnetic Tape ( ) Line Printer ( ) Cards ( )

9d. DISPOSITION OF DATA:

Return to Originator ( ) Library ( ) Destroy ( )

BE BRIEF – ELIMINATE UNNECESSARY WORDS

10. ORIGINATOR *(On separate lines, enter Name, Routing Symbol, & Tel. No.)*

11. DERIVATIVELY CLASSIFIED NSI NATIONAL SECURITY INFORMATION Unauthorized Disclosure Subject to Administrative and Criminal Sanctions
Derivative Classifier: (Name)
(Title)
Declassify on: (Date or Event/OADR)
Derivatively Classified by: (Guide or Source Document)

12. ORIGINALLY CLASSIFIED NSI NATIONAL SECURITY INFORMATION Unauthorized Disclosure subject to Administrative and Criminal Sanctions.
Originally Classified by: (Name)
(Title)
Declassify on: (Date or Event/OADR)

13. G RESTRICTED DATA- This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to Administrative and Criminal Sanctions.
DERIVATIVE CLASSIFIER _____
(Name and Title)

14. G FORMERLY RESTRICTED DATA- Unauthorized disclosure subject to Administrative and Criminal Sanctions Handle as Restricted Data in Foreign Dissemination Section 144.b Atomic Energy Act. 1954
DERIVATIVE CLASSIFIER _____
(Name and Title)

15. INSERT BELOW, CLASSIFICATION LEVEL, UNCLASSIFIED, OR OFFICIAL USE ONLY

Figure II-1. DOE F 1325.7A, Telecommunications Message (Data) (Page 1).

INSTRUCTIONS

(NOTE: More detailed requirements and instructions are contained in DOE 5635.1 and DOE 5300.1A. Procedures and illustrations for preparing this form are contained in the SACNET Users Guide.)

1. **and 15. Classification:** If the message is classified, stamp the 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. **Documentation:** Complete the documentation as required. Secret and Top Secret messages shall be documented in accordance with existing procedures. Series shall be assigned by the originating office as follows: Originating office copies – Series A Transmitting message center – Series B First addressee – Series C Each succeeding addressee – Series D, E, F, and so forth.

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:** See DOE 1325.1A for an explanation of message types.

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 in the signature block as a means of establishing the date time group for use in replies or future references 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.

9a. **through 9d:** (Refer to the special instructions for this form contained in paragraph 4.3.1 of the SACNET Users Guide.)

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 category stamp and complete the required information.

Figure II-1. DOE F 1325.7A, Telecommunications Message (Data) (Page 2).

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

2 Declassification/downgrading information **should** be placed on the visible marking, *if* such markings would apply to *all* of the classified information on the microfiche. If it will not fit, the declassification/downgrading information **should** be placed on accompanying documentation.

3 The classification level and category (if RD or FRD) and unique identification number (if applicable) **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.

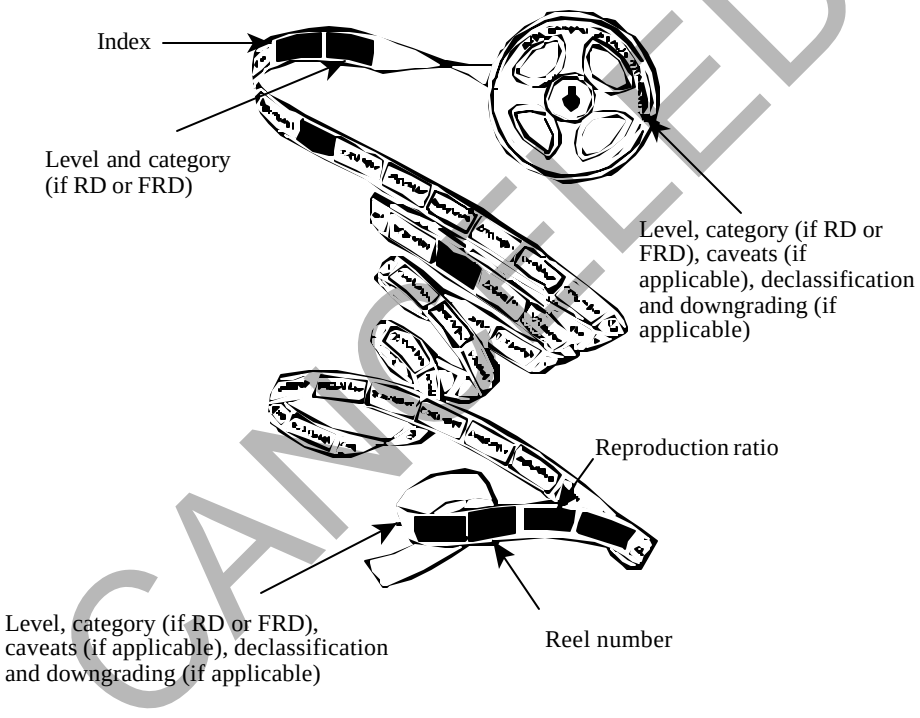
(g) Microfilm. Each microfilm reel **must** be marked on its face (i.e., on the reel itself) to reflect the classification level and category (if RD or FRD) and unique identification number (if applicable). See Figure II-2.

1 The first image **must** contain the highest classification level, category (if RD or FRD), and caveats (if applicable) of information. The face of the reel **must** reflect the highest level and category (if RD or FRD) of information contained on the microfilm.

2 Declassification/downgrading markings **must** be placed on the first image, *if* such markings would apply to *all* the classified documents on the microfilm. If it will not fit, then consider placing this information on accompanying documentation.

3 The second image **should** contain the reel number.

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



CLASSIFICATION FOR EXAMPLE PURPOSES ONLY

Figure II-2. Example Markings for a Classified Microfilm Reel.

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

6 The end of each reel **must** contain the highest level and category (if RD or FRD) of information on the 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 the unique identification number (if accountable). At the end of a film or video tape, the classification level **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).

The plastic or metal encasing the actual tape or film (i.e., the part placed into the recorder) **must** be marked to indicate 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 paragraph 3r, File Folders and Other Containers. See Figure II-3.

(7) Photographs. Roll negatives or positives **must** be marked at the beginning and end of each strip. Other markings **must** be applied to the reverse side or affixed by 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. 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.

(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

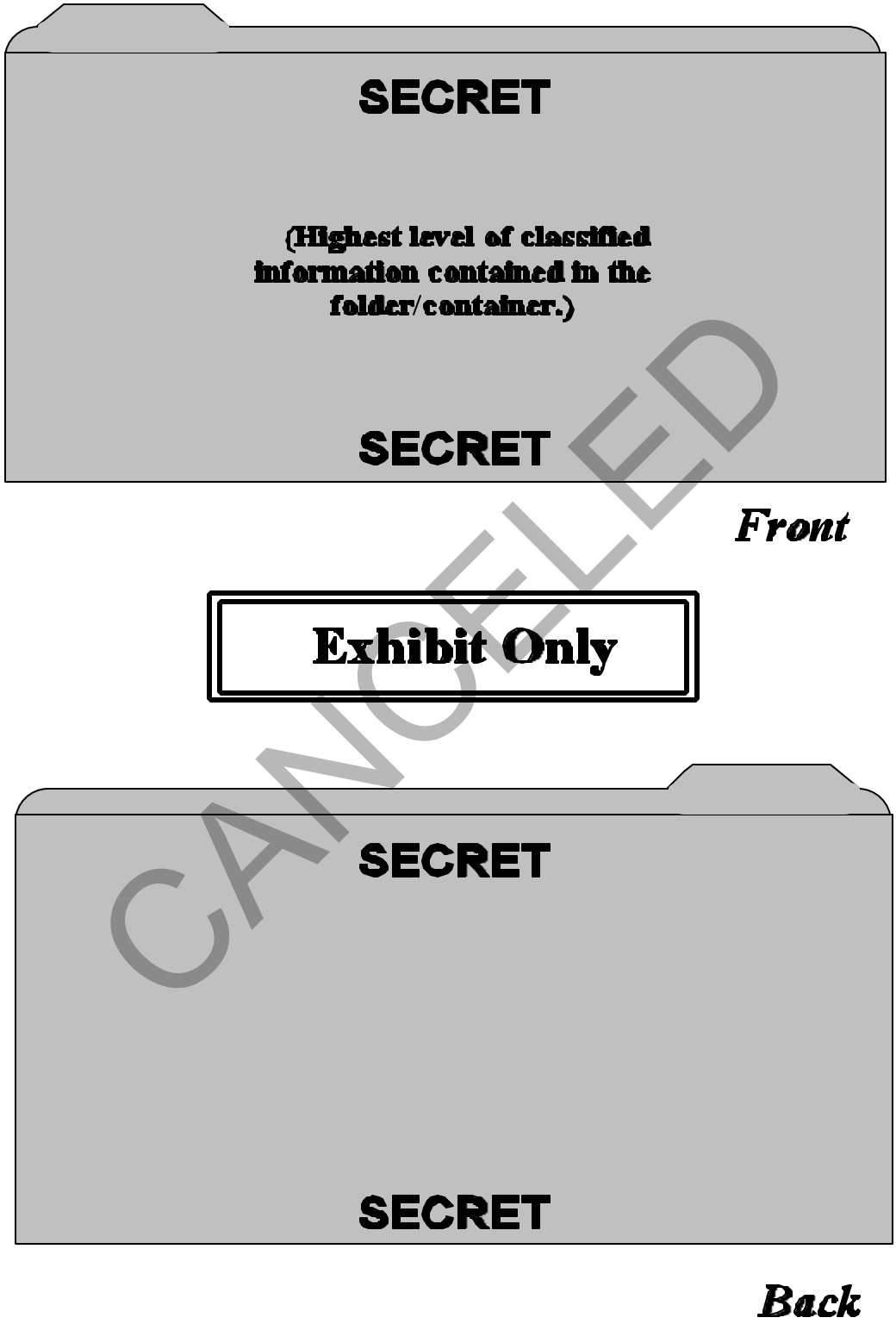


Figure II-3. Example Markings for Classified File Folders.

specified in this chapter **must** be shown on either the border or frame or in the accompanying documentation. The succeeding transparencies, slides, and sheet film **must** indicate, at a minimum, the classification level and category (if RD or FRD) and be shown on the image.

(b) When any portion or portions of a set of transparencies, slides, or sheet film are to be handled and controlled as separate documents, they require all standard markings.

(c) Each transparency, slide, or sheet film **must** 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), and the classifier information **must** be applied to the face of the recording by adhesive tape or similar material. The plastic encasing the actual tape or cassette (i.e., the part placed into the recorder) **must** be marked to indicate the classification level and category (if RD or FRD). Only the *removable* covering of a cassette or tape is considered a container and **must** be marked according to paragraph 3r, File Folders and Other Containers.

(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 media must have the overall classification level and category (if RD or FRD) visible on the front and back. Media must be marked using Standard Forms (SF-710 for unclassified, SF-709 for classified, SF-708 for Confidential, SF-707 for Secret, and SF-706 for Top Secret). Locally developed labels containing the information on the Standard Forms **may** be used. Classifier markings are not required on the exterior of electronic media.

When a platen or disk is removed from its manufacture's case, if it is not immediately destroyed, it must be marked with the classification level and category (if RD or FRD).

Labels that denote the classification level and category of the media may be used when it is practical to apply the label without impeding the operation of the removable media. If the label can impede the operation of the removable media, (e.g., not allowing the media to properly seat), then alternate marking methods are required. The classification markings **must** be visible and human-

readable, and **must** easily communicate the classification level and category 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.)

(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.

(14) Training Matter. Unclassified matter used to simulate or demonstrate classified matter for training purposes **must** be clearly marked to indicate that 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 in a manner to make it clear that 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 assists in distinguishing 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 in reduced size.

Table II-2. Foreign Equivalent Classification Markings.

Country	Top Secret	Secret	Confidential	Confidential FGI—Modified Handling Required
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
Bolivia	Supersecreto *or* Muy Secreto	Secreto	Confidencial	Reservado
Brazil	Ultra Secreto	Secreto	Confidencial	Reservado
Cambodia	Sam Ngat Bamphot	Sam Ngat	Roeung Art Kambang	Ham Kom Psay
Canada	Top Secret	Secret	Confidential	Restricted
Chile	Secreto	Secreto	Reservado	Reservado
Columbia	Ultrasecreto	Secreto	Reservado	Confidencial 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	ÁÊÑÙÓ ÁÐÏ ÑÑÐÔÏ Í	ÁÐÏ ÑÑÐÔÏ Í	ÅÌ ÐÉÓÔÅÕÔÉÊÏ Í	ÐÅÑÉÙÑÉÅÌ ÅÍ ÇÓ ×ÐÇÓÅÙÓ
Guatemala	Alto Secreto	Secreto	Confidencial	Reservado
Haiti	Top Secret	Secret	Confidencial	Reserve
Honduras	Super Secreto	Secreto	Confidencial	Reservado
Hong Kong	Top Secret	Secret	Confidential	Restricted
Hungary	Szigoruan Titkos	Titkos	Bizalmas	

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

Country	Top Secret	Secret	Confidential	Confidential FGI—Modified Handling Required
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	Secgretissimo	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
Laos	Lup Sood Gnod	Kuam Lup	Kuam Lap	Chum Kut Kon Arn
Lebanon	Tres Secret	Secret	Confidentiel	
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
Pakistan (Urdu)	Intahai Khufia	Khufia	Sigha-E-Raz	Barai Mahdud Taqsim
Paraguay	Secreto	Secreto	Confidencial	Reservado
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)	Hemlig	Hemlig		

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

Country	Top Secret	Secret	Confidential	Confidential FGI—Modified Handling Required
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 Pid
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	Ñîâåðøåííî Ñåêðåòíî	Ñåêðåòíî	Í å Ïîäëåæàùèé Î ãëàøåíèþ	Äëÿ Ñëóæåáíîãî Ïîëüçîâàíèÿ
Viet Nam (Vietnamese)	Toi-mat	Mat	Kin	Pho Bien Han Che

(16) Classified Page Changes.

(a) Periodic updates or revisions to a classified document **may** be transmitted as page changes instead of re-transmitting the entire document. When revising a classified document, the following three factors **should** be considered before deciding whether to transmit them as a new document or as page changes.

1 Do these page changes alter the current classification level and category?

2 Do these page changes replace the same number of pages without deleting needed information?

3 Is this an accountable document?

(b) If the revision does *not* alter the classification and replaces only outdated information, the revision **may** be sent as page changes. If the revision alters the classification or would remove needed information, the revision **may** be sent as a new document, or, if necessary, the entire document **may** be revised.

(c) Whether or not the document is accountable, the transmitting receipt for a page change **should** provide direction for incorporating the pages into the document.

1 If the classified document is non-accountable, the pages **may** be inserted and the obsolete pages destroyed properly.

NOTE: Non-accountable classified documents identified as requiring periodic updates or revisions **should** be entered into a tracking system to identify who has copies. This technique will allow page changes to be sent to the copy holders.

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 need not be given unique identification number**s**, a record of the page changes **must** be kept.

(d) Page changes **should** be marked in the same manner as the original document. For example: (1) If the original document was portion marked, the page change also **should** be portion marked and (2) If the

category was marked on each page of the original document, it also **should** be marked on each page of the page change.

r. File Folders and Other Containers. When not in approved secure storage repositories, 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-3.)

(2) Containers of classified documents such as videotapes or cassettes also **must** include classification level markings on the top and bottom of the front and back of the container. 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 as an inner envelope only, and address and mark them appropriately.

NOTE: The plastic encasing the actual tape or cassette (i.e., the part placed into the recorder) is not considered a container for the purposes of these marking instructions. Only the *removable* covering of a cassette or tape is considered a container.

s. Transmittal Documents. The first page of a transmittal document **must** be marked with the highest level 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 category and/or caveat spelled out; e.g., Restricted Data)*.

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

(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 inserted. (In this example, the level is Unclassified.)

When separated from enclosures, handle this document as (*insert classification level spelled out; e.g., Unclassified*)

(d) Good business practice suggests never stapling or binding a letter of transmittal to the classified document being transmitted. Such binding might imply that it is considered part of the document, which would change the marking requirements.

(e) If a letter of transmittal is separated from the document it has transmitted, good business practice suggests drawing a single line through the classification markings on the letter of transmittal and highlighting or circling the "When separated from enclosures, handle this document as Unclassified" marking. This technique helps reduce mistakes regarding the classification and handling of the letter of transmittal.

(2) Classified Letters of Transmittal. Classified letters of transmittal **may** 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.

OR

(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 below.

OR

(c) The final method, described below, allows for the letter of transmittal and the attached document to be transmitted together as one document but to be 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, the successive pages will 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 letter of transmittal has multiple pages, the successive pages will 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. If the category of the information in the transmitted document is higher, the 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, the category information marking **must** be placed on the lower left corner of the letter of transmittal.

(d) 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 _____," 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.

t. 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 need contain only the following markings:

(a) The date created.

(b) The highest potential overall classification level of the draft or working paper **must** be marked at the top and bottom on the outside of the cover page (if any), on the title page (if any), on the first page, 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 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 Papers" or "Draft" on the first page of text.

(e) Any applicable caveats or special markings **must** be annotated on the first page of text.

(2) Electronic versions of working papers and drafts are marked as required by paragraph q(3) of the chapter.

(3) Markings prescribed for a finished document **must** be applied when:

(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.

"Living documents" or "working papers" (i.e., documents being updated on a frequent basis as part of an ongoing experiment or study) **may** be considered to be originated each day that they are changed. Local procedures **must** provide a specific technique to demonstrate that the "living document" is in fact being changed frequently. A sheet attached to the front of the document that gives the number of pages and the date of the last posting is an example of such a technique.

(4) See Chapter II, paragraph 1e for instructions on documents pending classification review.

u. Redacted documents. Methods used to strike out classified information prior to release to persons not authorized access to the deleted information **must** completely obliterate the classified text, figures, etc., to prevent any form of recovery which **may** compromise the information. One method to ensure the complete removal of classified or other sensitive but unclassified information from a classified document in preparation for release is to copy the classified document and cut out the classified or other Sensitive Unclassified Information with a razor blade or X-acto® knife. Make a second copy of the document with the information removed.

v. Miscellaneous. Typewriter ribbon cartridges and spools or carbons **must** be marked with the appropriate classification level and protected accordingly until destroyed. No additional markings are required.

w. Other Government Agency and Foreign Government Documents Not Conforming to DOE Requirements. As a rule, documents received from other Government agencies and foreign governments that have not been marked to conform to DOE requirements need not be re-marked. However, as a minimum, all documents received **must** clearly indicate a classification level and category (if RD or FRD).

(1) Other Agency.

(a) If an accountable document arriving from another agency lacks a unique identification number, one **must** be assigned.

(b) When possible, avoid returning documents because of improper marking. Instead, call the sending site and attempt to resolve any marking issues.

(2) Foreign Government.

(a) Classified documents originated by a foreign government or international organization either retain their original classification level markings or are assigned appropriate U.S. classification level markings.

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 assigning a U.S. classification level marking, mark a document protector and place the foreign document inside, create a transmittal document for the foreign document, or place a sticker with U.S. markings on the foreign document. These practices will avoid marking up a foreign document which **may** have to be returned to the foreign government.

(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 afford a foreign government document.

x. Cover Sheets. Standard Form (SF) cover sheets **must** be applied to all classified documents when they are removed from a secure storage repository. SF 703 is the Top Secret cover sheet; SF 704 is the Secret cover sheet; and SF 705 is the Confidential cover sheet. Locally developed cover sheets of the same color and format as the standard forms **may** be used. Locally created cover sheets **may** be overprinted with classification category, caveats, and other information approved by the responsible security office.

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 a Limited Area (or higher).

(3) Any matter that requires accountability because of national, international, or programmatic requirements.

(a) Classified computer equipment and media supporting Nuclear Emergency Search Team (NEST) and Accident Response Group (ARG) operations.

(b) National requirements such as Cryptography (CRYPTO) and designated COMSEC.

(c) International requirements such as NATO ATOMAL, designated United Kingdom (UK) documents, or other FGI designated in international agreements.

(d) Special programmatic requirements (e.g., designated Special Access Programs and Sigma 14).

(4) Electronic storage media containing Sigmas 1, 2, 14 and 15 or a combination of nuclear weapons design/testing data.

(5) If any of the information stored in a safe is accountable, then the SF 700, Security Container Information, for that safe is also an accountable document. It does *not*, however, have to be placed into the *formal* accountability system;

it simply **must** be accounted for according to a reasonable written local procedure.

c. Control Stations. Control stations **must** be established and used to maintain records, 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.

d. 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. As 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). 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, etc.). 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. The unique document number (if a document) or unique serial number (if material). Unique identification numbers **may** be created either by creating a totally new number for each new document or 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 form of a unique number associated with it.

(4) Classification level (and category, if RD or FRD) and additional handling caveats, if any, of the matter.

(5) Disposition of the matter (e.g., destruction, downgrading, declassification, dispatch outside the facility, or incorporation into another accountability record) and the date. The term "disposition" varies in meaning as follows:

(a) Regarding origination, transmission, receipt, and reproduction, "disposition" means the offices or activities where the matter was distributed.

(b) Regarding destruction, "disposition" means the organization where the matter was destroyed and by whom.

(c) Regarding 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 on the associated paperwork.

(7) Number of copies of documents generated or reproduced and the disposition of each copy. The quantity of copies of a document made during either origination or reproduction.

(8) Authority for contractor retention. Contract or other written retention authority that authorizes the matter to be in the possession of a contractor, which **should** be readily available to facilitate compliance disposition reviews. 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.

(9) Date received, if applicable. The date the transmitted matter arrived.

(10) Activity from which the matter was received, if applicable. The office or activity name and address from which matter was transmitted to the recipient.

e. Inventory. An annual inventory of accountable matter **must** be conducted. Each item listed in an accountability record **must** be visually verified. All sites **must** develop procedures to ensure that all accountable matter has been entered into the accountability system. A report of unresolved discrepancies **must** be submitted in accordance with requirements for reporting incidents of security concern.

NNSA's NEST and ARG classified computer equipment and media will be inventoried at least once a month by two individuals. In addition, Albuquerque, Oakland, and Nevada will develop deployment and redeployment checklists for all ARG and NEST elements that include procedures for inventorying accountable equipment both before and after a deployment.

(1) Inventory records. Control stations **must** maintain records of the annual inventories and any reports generated as a result of the inventories (such as an unaccounted-for document report).

(2) Follow-up. Any discrepancies **must** be reported and dealt with according to DOE policy on reporting incidents of security concern.

f. 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 National Archives Records Administration (NARA) General Records Schedules.

(1) Secret and Confidential. This schedule requires the following for Secret and Confidential accountability records retention:

(a) Receipts. The receipt files that record the transmission or receipt of classified matter **must** be maintained for 2 years.

(b) Destruction. Destruction files **must** be maintained for 2 years after the date on which the documents are destroyed.

(c) Inventories. Forms, ledgers, or registers used to show identity, internal routing, or final disposition of classified documents (except for receipt and destruction record files) **must** be maintained for 2 years.

(d) Formerly accountable documents. Accountability records for documents formerly in accountability **should** be kept for 2 years after the documents are taken out of accountability.

(2) Top Secret accounting and control files.

(a) Registers maintained to indicate accountability of Top Secret matter (including transmission, receipt, and destruction) **must** be maintained for 5 years after the activity.

(b) Forms designed to ensure control of Top Secret matter, such as lists of names of persons handling the documents and intra-office routing slips, **must** be maintained until the associated document is downgraded or destroyed.

NOTE: Master files and data bases created in central data-processing facilities to supplement or replace Top Secret records are *not* authorized for disposal

under this general records schedule. These files **must** be scheduled on an SF 115, Request for Records Disposition Authority.

g. 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 treated as follows.

(1) Protected in accordance with the assigned classification.

(2) Destroyed when no longer needed.

(3) Accounted for (if required) and controlled in the manner prescribed for a finished document when the working papers and drafts are—

(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.

h. Automated Accountability Systems and Electronic Receipting

(1) General. Automated accountability systems are efficient and cost effective. As an administrative tool they are invaluable in terms of providing filing and retrieval capabilities. As a security tool, they can significantly add to the protection of and access control for matter. Several fully developed automated accountability systems exist within DOE. Several commercial products available on the market also meets DOE requirements. Some suggestions for successful implementation follow.

(2) Analysis. A thorough analysis is always the first step in developing an automated accountability system. Management **should** create an analysis team comprising, at least, computer experts, CMPC subject-matter experts, the CMPC Manager, and control station operators.

(3) Development. The analysis team **should** search for commercially available products and develop a program only if necessary. When evaluating products, the analysis team **should**—

(a) Ensure the software and hardware are compatible.

(b) Purchase state-of-the-art software and hardware to improve performance; normally, this also will save money in the long run.

(c) Consider programs/systems that have added security features (e.g., clearances, Sigma access).

(d) Consider administrative features such as automatic receipts, mailing labels, and optical storage of information.

(4) Budgeting. Budgeting **should** include not only purchase cost but also maintenance and training costs.

(5) Training. Develop or purchase a user-friendly training package. Insist that system users receive training *prior* to accessing the system.

(6) Loading Data. If possible, load data directly from the documents. Reconcile the new records with the old. Use bar-code labels, if possible; they are exceptionally accurate. Double-check and check again. Errors in data entry lead to enormous problems that require expensive solutions.

(7) Combined Systems. It is possible, and sometimes preferable, to combine accountable and non-accountable documents into one system.

(8) Electronic Receipting. The Information Security Oversight Office has approved in concept the use of electronic receipting systems, as long as the following conditions are met. The systems **must—**

(a) be approved by the local DOE operations office,

(b) provide identification of both the individual and the document disposition, and

(c) provide adequate security to ensure access control.

(9) Control Measures. The following control measures **may** be used to enhance the control of classified matter.

(a) Administrative tracking systems. Consider the appropriateness and cost effectiveness of establishing a system for administrative tracking of classified and unclassified documents. Such a system often is a good business practice in situations involving large quantities of documents that are used on a regular basis.

(b) Centralized holding areas. Consider consolidating classified matter as much as possible, operationally efficient, and economically feasible.

This technique facilitates control and protection of the matter. It also might save money in the long run.

(c) Internal receipting. Consider using receipts for documents being transmitted within a facility. A facility that is spread out over a large geographical area, for example, could benefit from an inexpensive internal receipting policy.

(d) Control of classified copiers and shredders. Establishing strict controls over the locations of classified copiers and shredders, over who can use them, and under which conditions helps maintain proper protection and control of documents. For example, the use of key codes for copiers and shredders provides improved access control to these machines, which improves document protection and control.

(e) Access control. Vigorous enforcement of access control procedures also assists in maintaining proper protection and control of matter. With the creation of security islands and increased use of automatic access-control systems (such as card readers and optical scanners), individuals **should** be more aware of the potential for unauthorized personnel to gain access to limited areas.

(f) Security awareness. Reduced accountability requirements and reconfigured security areas **should** be balanced by a proportionate *increase* in individual security responsibility. Because the reduction in administrative requirements also decreases the visibility of the CMPC program, security awareness becomes more important to the overall security program. Creating a security-conscious work environment is critical. The way to accomplish this goal is to instill in every employee a sense of personal responsibility for security.

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. If a classified document needs to be copied immediately and the document contains a caveat limiting reproduction without originator approval, the following procedure **may** 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.

(c) Follow up by obtaining permission in writing as soon as possible.

(2) Departmental elements and contractors **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) The Originator Controlled (ORCON) caveat marking is used to restrict reproduction to that allowed by the originator. Because this is a Director of Central Intelligence marking, it is to be used for intelligence documents only.

(b) Originators of nonintelligence documents who wish to prevent unlimited copying of a classified document **may** use the markings, or one similar in content, specified in paragraph 3l(1) of this chapter.

(3) Reproduction **must** be accomplished by authorized persons who know the procedures for classified reproduction and only in the performance of official or contractual duties.

(4) Reproduced copies are subject to the same protection and control requirements as the original.

(5) Reproduction restrictions **must not** restrict 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 of this chapter.

b. Equipment. Classified documents **must** be reproduced on equipment specifically approved and designated for such purpose to ensure minimal risk of unauthorized disclosure. To the greatest extent possible, these machines **must** be located within Limited Areas, Protected Areas, or Exclusion Areas. Technology that prevents, discourages, or detects the unauthorized reproduction of classified documents is encouraged.

(1) Access to Machines. Reproduction of classified information **must** be accomplished under appropriate security conditions to preclude unauthorized access to classified information. Classified copying **must not** be performed in the presence of either uncleared persons or persons without the proper clearance level.

(2) Notices. Notices regarding the restrictions and requirements of reproducing classified information **must** be posted conspicuously next to the equipment. See Figures II-4 and II-5.

(3) Clearing. Ensure that no classified waste is trapped or left in the equipment; clear all possible residual classified images after classified reproduction. Local procedures and the design of the copier will dictate how the copier will be sanitized.

(4) Approval. Ensure that all machines to be used for reproducing classified documents are approved for classified reproduction by the Facility Security Officer (FSO) or designee. Any CMPC program operations manager responsible for gaining approval of copy machines **should** obtain technical assistance from the Classified Information Systems Security or Technical Surveillance Countermeasures offices. At a minimum, ensure the following:

(a) classified copy machines do *not* have modems or the capability to be connected to an external modem.

(b) contracts for new digital copy machines specify that the memory chips will *not* be removed without permission and any remote diagnostics capabilities will be disabled.

c. Documents to or from Outside Agencies.

(1) Sending Documents. When DOE classified documents are transmitted to outside agencies, the documents **may** be reproduced without consent, unless they are marked with a caveat limiting further reproduction.

(2) Receiving Documents. DOE employees **may** reproduce outside agency documents in accordance with the same rules and restrictions that exist for DOE documents, unless specific instructions to the contrary accompany the documents. For example, National Security Council documents will have a copy restriction notice; therefore, National Security Council documents will be reproduced only with the permission of the originator.

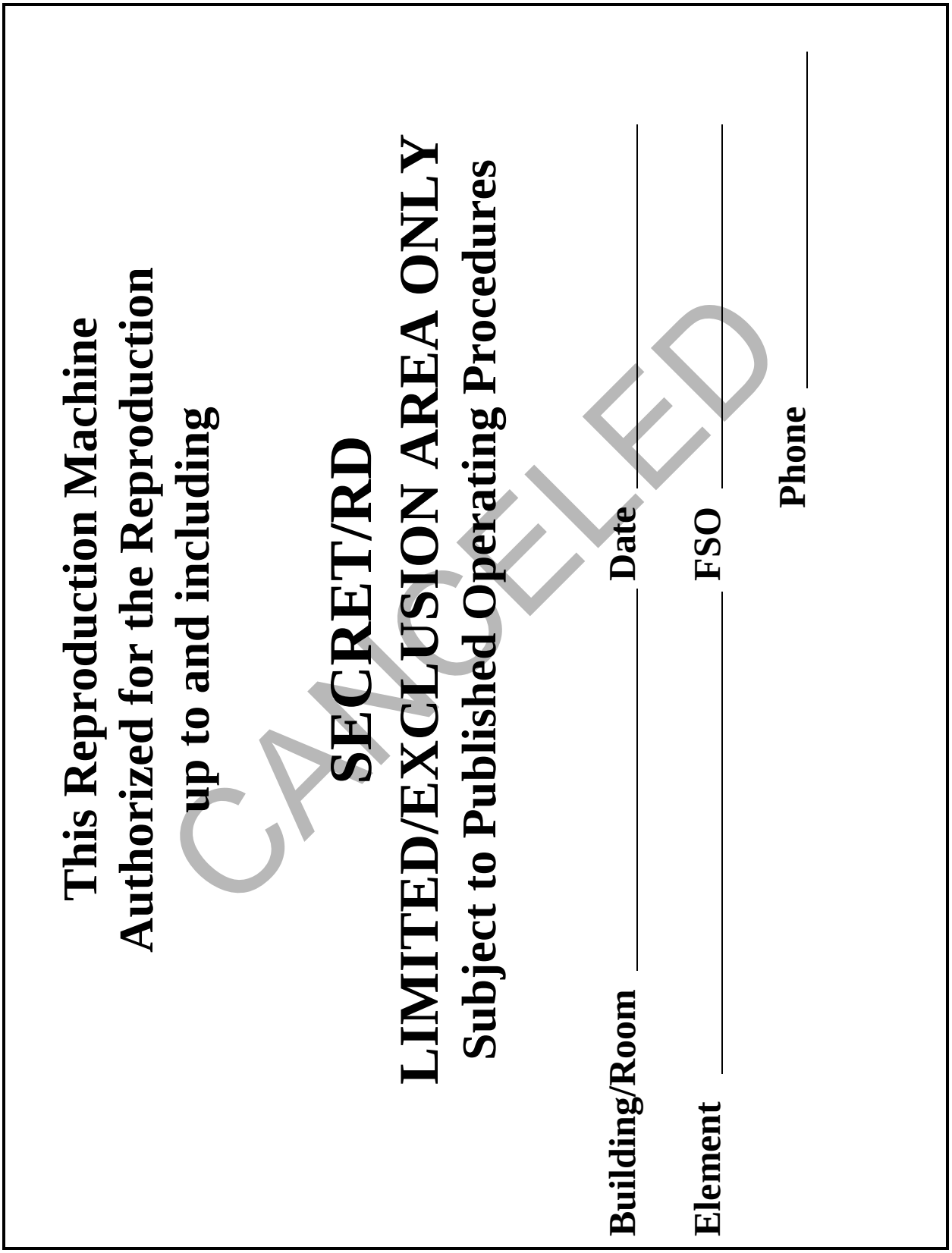


Figure II-4. Notice Regarding Restrictions on Reproducing Classified Information.

CLASSIFIED REPRODUCTION PROCEDURAL INSTRUCTIONS (Within Limited/Exclusion Area)

1. See AUTHORIZATION POSTER for classification limits and restrictions.

2. Observation of classified operations limited to persons with appropriate clearance and need to know.

3. Reproduction authorization required for ORCON or other control caveats which limit or prohibit reproduction without specific permission.

4. Limit number of copies to only that which is absolutely required. If in ACCOUNTABILITY, all copies must be brought under control.

5. Unacceptable or excess copies MUST be destroyed as classified information (accountability and destruction receipts not required).

6. After copying operations are completed, run (required number) blank copies through the machine and check the last copy for images. If images are still present, continue 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 are collected).

Figure II-5. Classified Reproduction Procedural Instructions.

6. RECEIPT AND TRANSMISSION.

a. General. Classified matter **must** be transmitted only in the performance of official and 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 contracting Departmental element 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.

(1) Classified matter **must** be delivered with the inner envelope unopened to personnel designated to receive it at a control station. 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 before delivery to the control station. Though the inner envelope **must not** be opened prior to arriving at the control station, the outer envelope **may** be opened prior to arriving at the control station, 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 reported promptly to the cognizant DOE safeguards and security office. If the matter was received through the U.S. Postal System, 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) When envelopes are used for packaging, the classified information **must** be protected from direct contact with the inner envelope. The inner envelope **must** be sealed and marked with the recipient's and the sender's classified addresses (i.e., mailing, shipping, or overnight); the overall level and category (if RD or FRD) of the contents; and any appropriate caveats. The outer envelope **must** be sealed and marked with the recipient's and the sender's classified

mailing addresses. The outer envelope **must not** carry markings indicating that the contents are classified.

(a) Containers.

1 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.

2 Protection of classified information from direct contact with the inner envelope is accomplished by having a cover sheet on the front of the document, and a sheet of paper or a cover sheet to protect the back of the document if the document contains information on the back page.

3 All the seams of an envelope or wrapper **should** be sealed with tamper-resistant tape (e.g., fiber tape) to prevent undetected access to the contents while in transit. When interpreting how much effort **should** be put into sealing the envelopes, consider why double wrapping and seals are required: to prevent easy and undetected access to the classified information while in transit. Also remember that U.S. Postal Service regulations require that all registered packages be sealed with paper tape.

(b) Inner containers. The classification level **must** be marked on the top and bottom of the front and back of the inner container. The category (if RD or FRD) and any caveats or special markings, of any of the matter, **must** be placed on the front of the inner container. The sender's classified address **should** appear in the upper left corner. The recipient's address **should** be centered on the envelope.

(2) 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. 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. 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. 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. The outer container **must** be addressed to a classified address, return addressed to a classified mailing address, and sealed with no markings to indicate that the contents are classified.

(3) 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 as 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 that the contents are classified.

(4) If the classified matter is an inaccessible internal component of a bulky item of equipment that cannot be reasonably packaged, such as a missile, no inner container is required and the outside shell or body **may** be considered as 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.

(5) If specialized shipping containers, including closed cargo transporters, are used for transmitting classified matter, the container **may** be considered as the outer container. 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. 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.

(6) If a locked briefcase is used to hand-carry classified matter of any level, the briefcase **may** serve as the outer container. The inner container **must** be sealed, addressed with the sender's and recipient's classified address, and marked with the overall level and category (if RD or FRD) of the contents and with any appropriate caveats. The briefcase (outer container) **must** indicate the return classified address and **must** contain no markings to indicate that the contents are classified. A briefcase cannot serve as the outer container for travel aboard commercial aircraft. The requirement that an individual carrying a briefcase with classified matter outside a security area **must** possess a DOE 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.

d. Receipts. For all accountable and Secret matter, DOE F 5635.3, Classified Document Receipt, or a receipt comparable in content, **must** be used to transmit 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 it **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 Figure II-6 for a copy of DOE F 5635.3.

(1) Exceptions. Receipts are not required for non-accountable classified matter under the following conditions:

(a) transmission of matter within a facility and
(b) transmittal of Confidential matter.

(2) Facsimile Transmission. Individuals transmitting classified information through facsimile systems **must** confirm receipt (written or verbal) with the intended recipient. A receipt such as DOE F 5635.3, or one similar in content, **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. Another 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 that the complete transmission was received. This verbal communication must be documented and retained and will suffice for all other written forms of a receipt.

(3) 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, any receipt that is submitted **must** be signed and returned to the sender.

(4) Suspense Copy. 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 suspense date (normally not to exceed 30 days) **must** be established, and follow-up action **must** be initiated if the signed receipt, or similar written confirmation, is not returned within the suspense period. 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. Copies of signed receipts for classified matter **must** be retained at control stations in accordance with the DOE Records Schedule and the NARA General Records Schedules. Procedures **should** be established for both tracking the return of receipts and the actions required if receipts are not returned.

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	CLASSIFICATION (Indicate whether or not RD, FRD, or NSI)	COPY and SERIES	NUMBER of PAGES

I have received the document(s) listed above and assume responsibility for safeguarding in accordance with security regulations.

Signature of addressee or name of addressee and signature of recipient. _____ *Date* _____

Received for addressee by _____ *Date* _____

(to be used only by mail rooms)

1. Return to Sender 2. Addressee's Copy 3. Pending Copy

V Printed with soy ink on recycled paper

Figure II-6. DOE F 5635.3, Classified Document Receipt (Page 1).

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, DC 20585; and to the Office of Management and Budget (0MB), Paperwork Reduction Project (1910-1800), Washington, DC 20503.

Figure II-6. DOE F 5635.3, Classified Document Receipt (Page 2).

(5) 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 and sent to the intended recipient. The third copy **must** be maintained by the sender until the original is signed and returned. The receipt **should** contain the following information:

(a) the full names of the sender and the recipient;

(b) the address of the sender;

(c) the classified address of the recipient;

(d) a description of the classified matter (e.g., title or other means);

(e) the date of the matter;

(f) the classification of the matter; and

(g) the unique identification number, if applicable.

(6) 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 address in the Safeguards and Security Information Management System (SSIMS).

(7) Electronic Receipting. The Information Security Oversight Office has approved the use of electronic receipting under the following conditions:

(a) The system **must** provide a method to ensure that individuals authorize the use of their electronic signature for any transaction.

(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.

e. Classified Addresses.

(1) Classified matter **must** be addressed only to approved classified addresses (i.e., mailing, shipping, or overnight delivery) contingent upon the appropriate method of transmission.

(2) Classified addresses **must** be verified through SSIMS and are valid for 30 days from the date of validation. The SSIMS contains the data from each facility's approved Facility Data and Approval Record, which identifies the approved

classified address. Only five lines are available to record classified mailing addresses. Alternative methods for verifying classified addresses are to contact either the responsible DOE security office or Assessments and Integration of the Field Operations Division (SO-212.1) at DOE Headquarters.

(3) 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.

(4) 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.

(5) Mail addressed as indicated in subparagraph (4) above **must** be delivered only to the addressee or to 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.

f. Receipt and Transmission Within Facilities. Classified matter transmitted within a facility **must** be prepared to ensure adequate security protection for the classification 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—

(a) personnel who have appropriate access authorization for the classification level and category of classified information involved or

(b) approved electronic means.

(2) Wrapping. Although double-wrapping is *not* required for classified matter transmitted within a facility, the transmission 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 **should** be covered by some form of protective covering to preclude unauthorized view.

(b) If the classified matter is transmitted by the site delivery personnel, it **should** be placed within a container to prevent exposure during transfer.

(3) Electronic Means. Classified matter **may** be sent by an approved electronic means. When using this method, ensure that both the transmitting and receiving systems are approved in a manner commensurate with the classification level and category of the information to be transmitted. The system also **must** have an approved security plan and procedures for transmitting the information.

g. 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,* for secure communications requirements.

(3) Individuals **may** be authorized to hand-carry Top Secret matter in accordance with paragraph 6j of this chapter.

h. 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 **may** be transmitted through the following postal 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. The use of the U.S. Postal Service is not permitted for the transmission of Communications Security (COMSEC) material or COMSEC keying material; see DOE M 200.1-1, *Telecommunications Security Manual,* for approved methods of transmission. A return mail 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 that approval is obtained from Headquarters Office of Safeguards 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 by Canadian registered mail with registered mail receipt in transmitting matter to and between U.S. Government and Canadian Government installations in the 50 states, the District of Columbia, and Canada.

(3) Approved commercial express service organizations **may** be used to transmit Secret matter in accordance with the provisions contained in paragraph 6k of this chapter.

(4) Approved common carrier services with escorts who possess the appropriate access authorization **may** be used to transmit Secret matter in accordance with paragraph 6l upon approval by the cognizant DOE safeguards and security authority.

i. 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 and registered mail. NOTE: Other Government agencies **may** use First Class mail; use of First Class mail is not authorized for DOE.

j. Authorized Hand-Carriers. The following requirements apply to individuals approved to hand-carry classified matter; however, the requirements identified in paragraph 6l also apply to hand-carrying of bulk documents.

(1) The cognizant Facility Security Officer identified on DOE F 5634.3, 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

appropriate protection measures are implemented. A record of the classified matter **must** be made prior to departure. A copy of the record **must** be carried by the employee. On the employee's return 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—

(a) an unusual situation warrants such action;

(b) the classified matter is not available at the destination;

(c) the time does not permit transmission by other authorized methods;

(d) the classified matter can be properly handled and protected during transmission;

(e) the transmission can be successfully completed on the same day;

(f) the classified matter can be appropriately stored 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 DOE security office.

(2) Contingency plans for delayed arrival **must** cover alternative protection and storage procedures and reporting requirements. Site contingency plans **may** be placed in locally developed procedures, as long as they are approved by the cognizant DOE security office. Generic plans **may** be developed for different potential contingencies and used as necessary. Sites are not required to develop specific contingency plans each time a person hand-carries classified matter.

(3) 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) Authorization. Individuals designated to approve employees to hand-carry or escort classified matter **must** be designated in writing. This authority **should** come from upper management and be limited to as few people as operationally feasible.

(b) Authorized Hand-Carriers. The site **must** be able to identify individuals authorized to hand-carry. This **may** be accomplished by maintaining training records.

(4) Only the classified matter absolutely essential for the purpose of the visit or meeting **may** be hand-carried by the employee.

(a) 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 safeguard classified information.

(b) 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. 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.

(c) Arrangements **must** be made in advance of departure for overnight storage at an approved facility that has appropriate storage capability.

(5) 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 Director, Headquarters, Office of Safeguards and Security. The authorization to hand-carry classified matter outside the United States is strongly discouraged and will 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 Director, Headquarters, Office of Safeguards and Security.

(c) Individuals authorized to hand-carry classified matter outside the United States **must** possess a "Non-Professional Courier Letter," signed by the Director, Headquarters, Office of Safeguards and Security.

(6) Classified matter **may** be hand-carried aboard commercial passenger aircraft by cleared employees with the approval of the cognizant Facility Security Officer. Classified matter that can be subjected to routine airport security measures without providing access (i.e., paper documents) does not require notification to airline or airport security personnel. When the classified matter would be compromised if subjected to routine airport security measures, the guidance provided in FAA Circular AC 108-3, "Screening of Persons Carrying U.S. Classified Material" **must** be followed. See Figure II-7 for a copy of Federal Aviation Administration Circular 108-3.

(7) X-Ray Screening of Documents. When classified documents are in small containers, the traveler **should** report to the airport screening station where the package will be routinely inspected by x-ray. If the screening official inquires about the contents of the package, the traveler first **must** display the travel authorization and appropriate identification and then **must** explain to the screening personnel that the package in question is classified.

(8) X-Ray Screening of Material. If the physical characteristics of the classified material would reveal classified information, the traveler **must** have a letter of authorization to preclude x-ray screening at the air terminal. According to FAA Circular 108-3, the authorization letter **must** include the following information (see Figure II-8 for an example):

(a) full name and company;

(b) type of identification the traveler will present;

(c) physical description of the container to be carried;

(d) points of departure, the destination, and any known transfer points;

(e) effective and expiration dates, not to exceed 7 days from the date of issue;

(f) name, title, signature, and telephone number of official issuing the letter and matching signature on the face of each container to be exempt from screening; and

(g) name and telephone number of the responsible security office that can verify the classified nature of the matter.

AC 108-3

11/6/81

ADVISORY CIRCULAR

Department of Transportation
Federal Aviation Administration

FAR GUIDANCE MATERIAL

Subject: SCREENING OF PERSONS CARRYING U.S. CLASSIFIED MATERIAL

1. PURPOSE. To provide instructions for the screening of passengers carrying classified material in order to maintain the integrity of the screening process and prevent the compromise of classified material.

2. BACKGROUND. On occasion, personnel of the Federal Government and personnel of contractors to the Federal Government have a need and are authorized to carry material containing information classified in the interest of the national security. Due to the requirements of the Federal Aviation Regulations, all passengers and their carry-on items must be screened prior to boarding scheduled air carrier aircraft. Carry-on items which contain classified material (matter), if routinely examined, could subject the information to compromise.

3. CLASSIFIED MATERIAL SCREENING PROCEDURES. Persons carrying Government classified materials shall be screened in the same manner as other passengers except for the following:

a. The passenger should inform the carrier representative classified materials are being carried and should present an official U.S. Government or company identification and travel documentation. In most instances, the classified materials being carried will be contained in sealed envelopes or small packages. In these instances, the passenger is to report to the screening station for routine processing. At that point, the classified material shall be processed by X-ray examination where such equipment is available and where such processing is feasible. The classified material shall contain no metal bindings and shall be in sealed envelopes or packages. If the envelopes/packages containing the classified material, the passenger's other carry-on baggage and the passenger successfully complete the required screening, the passenger shall be permitted to board. Where there is no X-ray equipment in use, the person screening the carry-on baggage should be able to inspect envelopes containing classified material to assure the absence of weapons by flexing, feel, weight, etc., without opening the envelopes. In the event that the person

Figure II-7. Advisory Circular (Page 1).

conducting the screening is not satisfied and there is doubt as to the contents of the envelopes, the passenger shall not be permitted to board with the envelopes. Opening of the envelopes containing classified material by screening personnel is not authorized and should never be attempted.

b. In a few instances, classified material will be in sealed packages which, because of size, weight, or other physical characteristics, are not suitable for processing as specified above. Persons carrying such material shall be screened in the same manner as other passengers, except for the following:

(1) Federal Government or contractor official who has authorized the transport of the classified material shall notify an official of the appropriate air carrier in advance of the travel. Upon notification, the carrier should advise the authorizing official that the courier should be instructed to report to the airline ticket counter upon arriving at the air terminal. Upon arrival at the ticket counter, a carrier representative shall check the courier's identifying documents.

(2) Federal Government and contractor personnel shall present an identification card or credential bearing a photograph, description data, and signature of the individual. (If the identification card does not carry descriptive data, i.e., date of birth, height, weight, or signature, these items. must be included in the courier letter of authorization described below.) Federal personnel will present official identification issued by their agencies. Contractor personnel will present identification issued by the contracting firm or company employing the individual or an identification issued by the U.S. Government. In the latter instance, the identification card will carry the name of the employing contractor or otherwise be marked to denote "contractor."

(3) Federal Government and contractor personnel shall also present the original of a letter authorizing the individual to carry classified material. A reproduced copy is not acceptable. The letter may contain a preprinted endorsement for authentication by an official at the destination in cases in which round-trip carrying is involved. The traveler however, shall provide an authenticated copy to each airline involved. The letter should be prepared on letterhead stationery of the agency or contractor employing the individual. In those instances where an individual visiting another agency of a contractor is given classified information which he/she must transport by return trip and has not letter from

Figure II-7. Advisory Circular (Page 2).

his/her organization covering the material, the letter of authorization will be prepared on the letterhead stationery of the agency or contractor being visited. The letter of authorization should:

(a) Give the full name of the individual and the employing agency or company.

(b) Describe the type identification the individual will present (e.g., Naval Research Laboratory Identification Card, No. 1234, ABC Corporation Card, No. 1234).

(c) Describe the material being carried (e.g., three sealed packages, 9" x 18" x 24", addressee, and addressor).

(d) Identify the point of departure, destination, and known transfer points.

(e) Carry a date of issue and an expiration date not exceeding seven days from the date of issue.

(f) Carry the names, title, signature, and telephone number of the official issuing the letter. Each package or carton to be exempt will be signed on its face by the official who signed the letter.

(g) Carry the name of the Government agency designated to confirm the letter of authorization and its telephone number. The telephone number of the agency designated shall be a U.S. Government official number that is subject to verification for both Government and contractor use.

(4) If satisfied with the identification and the letter of authorization, the carrier representative shall provide the passenger with an escort to the screening station and authorize the screening personnel to exempt the classified packages from physical or other type inspection. The passenger and all other items the passenger may be carrying shall be subject to normal screening. If the airline representative is not satisfied with the authenticity of the passenger or the documentation presented, he/she should contact a representative of the authorizing official for appropriate verification. If the airline representative is still not satisfied, the passenger shall not be permitted to carry the classified packages aboard. In these instances, the U.S. agency or company involved

Figure II-7. Advisory Circular (Page 3).

4. ARMED FORCE COURIER SERVICES (ARFCOS)SCREENING PROCEDURES. The ARFCOS has been specifically designate by the Department of Defense to escort courier material classified TOP SECRET that is considered highly sensitive by the Federal Government. All branches of the Federal Government and qualified contractors of the Government may be served by ARFCOS in the transportation of these types of materials.

a. In most instances, material in the custody of ARFCOS courier will be of such volume as to require loading in the aircraft cargo compartment. The loading of this material will be under the supervision of a representative of the carrier, but it must be accompanied by and under constant surveillance of ARFCOS personnel who will remain on guard until the cargo compartment is secured. In accordance with Air Transport Association policy, air carriers will normally accept ARFCOS Forms 9 and 14 as authorization for ARFCOS couriers to gain access to sterile ramp areas. The ARFCOS courier will be the last passenger to board the aircraft and the first to deplane. Off-loading procedures will also be observed by the ARFCOS courier. The carrier concerned will be given sufficient advance notification by the dispatching Armed Forces Courier Station in order that arrangements for transporting the courier material to the aircraft can be completed.

b. Hand-carried ARFCOS material will be placed in an ARFCOS courier pouch then secured with an ARFCOS lock. Screening procedures as outlined in 3 above will be followed.

c. ARFCOS courier personnel are not armed and may or may not be in military uniform. All such persons will be identified by both their military and an ARFCOS identification card (ARFCOS Form 9, buff with a red stripe, or Form 14, blue with a red stripe) in addition to the prescribed letter of authorization.

d. It is incumbent upon the courier to assure that appropriate arrangements are made at the destination for secure storage of classified material as may be required.

Figure II-7. Advisory Circular (Page 4).

Department of Energy
Central Training Academy
P.O. Box 5400
Albuquerque, New Mexico 87115

Airline and Airport Security Officials
Washington National Airport
Washington, DC 20003

SUBJECT: Letter of Authorization

This is to certify (*name of traveler*), who is an employee of (*name of employer*), is hereby authorized to hand-carry U.S. Department of Energy classified matter between (*identify point of departure, destination, and known transfer points*). This authorization is effective (*date*) and expires (*date - not to exceed 7 days*).

(*Name of traveler*) will produce, upon request, a photo identification badge issued by (*name of employer*), which contains descriptive information and his/her signature.

(*Name of traveler*) is hand-carrying this information in the performance of official duties and is not authorized to open the package(s) which are (*describe the package(s)*) for visual inspection of its contents by airport officials. The package can be further identified by a matching signature of the signer of this authorization on the face of the package(s). It is hereby certified that the package(s) does not contain hazardous materials.

Should you have any questions, please contact the undersigned, who is a U.S. Department of Energy security representative, at (*area code and number)*.

Seymour Findings
Director of Information Security

Figure II-8. Example Letter of Authorization.

(9) Advance Notification of Air Carrier. When the classified package precludes x-ray screening, the traveler **should** notify an official of the air carrier in advance that the package is to be transported.

(a) The traveler **should** report to the airline ticket counter upon arriving at the terminal and display the original letter of authorization and identification. Reproduced copies are not acceptable.

(b) Upon acceptance of the authorization, the air carrier representative will escort the traveler to the screening station and exempt the parcels from screening.

(c) The traveler and all other items carried **must** be subject to normal screening. If the air carrier representative is not satisfied, he or she **may** contact the responsible security office for verification. **Should** the screening personnel insist on opening the package, the traveler **must** decline to board. Under *no* circumstances **will** the traveler permit visual inspection of classified matter by screening personnel.

(10) Records. A record of all accountable classified matter to be hand-carried **must** be maintained both at the facility and with the individual transporting the matter. Receipts **must** be prepared in accordance with paragraph 6d of this chapter. The record **should** contain the following information:

(a) subject or title,

(b) date of the matter,

(c) date the matter was removed from the facility,

(d) signature of the person removing the documents, and

(e) the date the matter is 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 facility(ies) on the next working day. Commercial express service **must not** be used as a matter of routine or convenience for transmitting classified matter.

(1) As a minimum, the sender **must** ensure the following conditions are met:

(a) The express service organization has been approved by the Office of Safeguards and Security.

(b) The transmittal address, identified in SSIMS as the Overnight/ Classified Common Carrier Address, is used on all wrappers.

(c) The intended recipient(s) is notified of the proposed shipment and arrival date.

(d) All packages are double-wrapped before being inserted into the packaging provided by the commercial express service organization.

(e) The properly wrapped package is 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) Since 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 recipient that someone will be available at the facility(ies) to receive the shipment on arrival.

(2) Federal Express. Federal Express currently 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 operations office and are listed in SSIMS.

(a) In accordance with manual packaging requirements, Federal Express packages **cannot** be identified as classified shipments either by telling Federal Express employees or by marking the outer package as classified.

(b) The packaging provided by the commercial express service organization provides the best protection of the classified matter and is recommended over the use of other packaging material.

(c) 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 and *cannot* be a post office box, but **must** be a street address. Do *not* use terms such as "Document Custodian" in the address; however, the custodian's name **may** be used.

(d) Operations offices 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.

(e) Prior to establishing an address, operations offices **should** review internal local procedures to ensure that packages are opened only by appropriately cleared personnel.

(f) Federal Express business locations **must not** be granted DOE facility clearances and its employees **must not** be processed for personnel security clearances. Facilities **should** include specific details regarding the use of Federal Express in local procedures.

(g) The sender **should** provide the recipient with the air bill number for tracking purposes. All packages can be tracked 24 hours per day by using tracking software available through Federal Express.

(h) The use of Federal Express drop boxes for classified shipments is prohibited.

(i) Federal Express offers overnight freight service for packages weighing 150 to 750 lbs. Packages weighing more than 750 lbs require prior notice. Contact the local Federal Express office for details.

(j) If there are any problems noted with any classified Federal Express delivery, contact the Headquarters CMPC Program Manager immediately. Any delays in notification will directly affect the ability of the program manager to correct the identified problem.

l. Common Carrier Services. Common carrier services include all modes and means of transport (including, air, rail, vehicular, intra-city messenger services, etc.), excluding express service organizations. The following requirements apply to the use of such commercial services, as well as bulk shipments of classified matter:

(1) Contents **must** be securely packaged and **must** meet applicable regulations (including those of the Department of Transportation).

(2) 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 local safeguards and 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.

(a) Whenever practicable, combination padlocks meeting Federal Specification FF-P-110 **must** be used to secure closed cargo areas of vehicles, vans, and railroad cars.

(b) 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.

(3) Assurances and Notifications.

(a) The carrier **must** have a facility clearance in accordance with DOE O 470.1, *Safeguards and Security Program,* and a favorable Foreign Ownership, Control, or Influence determination.

(b) Notification of shipments **must** be transmitted to the consignee prior to departure with sufficient time to enable proper handling at the destination. As 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 transshipping activities personnel. Upon receipt of such notice, the consignor **must** immediately begin tracing the shipment.

(4) 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) As 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 when storage is required, an alarmed or guarded storage area with immediate response by a carrier employee, commercial guard, or police officer.

(c) When shipments are transported by rail, personnel escorting the shipment **must** travel in an escort car accompanying the shipment, keeping the shipment car(s) under observation. When practicable and time permits, personnel escorting the shipment **must** check the car(s), 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 shipment **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 vehicle. During stops or layovers, personnel escorting the shipment **must** check the tamper-indicating devices and locks.

(e) The identity and authorization of person(s) who pick up the classified matter **must** be verified.

7. CONTRACT CLOSEOUT/FACILITY 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, destroyed, or retention is authorized. DOE O 470.1, *Safeguards and Security Program*, and this Manual, state that Departmental elements will develop procedures; therefore, the details of contract closeout and facility termination are in local safeguards and security procedures.

b. Contract Completion. Upon completion or termination of a contract, the contractor **must** submit to the contracting officer either a certificate of nonpossession or a

certificate of possession. The contracting officer **must** then transmit the certification to the cognizant security office.

c. Certificate of Nonpossession.

(1) Upon return or destruction of all classified matter pertaining to a contract, the contractor **must** submit a certificate of nonpossession to the cognizant DOE security office. The certificate **must** include the contract number and a statement that all classified matter has been returned or destroyed.

(2) When a Departmental element's facility clearance is to be terminated, a certificate of nonpossession **must** be completed as part of the facility termination process. When a contract is completed, the contractor usually destroys or returns all classified matter, unless it provides a benefit to DOE to retain the classified matter. The format of the certificate of nonpossession is up to the responsible contracting office. Suggested formats are letter, memorandum, or local form. See Figure II-9 for an example of a certificate of nonpossession. For specifics on how to ensure that the certificate of nonpossession is accurate, see the guidance in paragraph 7e, Termination of Facility Clearance.

d. Certificate of Possession.

(1) 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, the type or form, and the quantity.

(2) If the classified matter will aid the U.S. Government in performing another active contract and the matter is being transferred to the active contract, the contractor **must** provide the Departmental element or the other Government agency 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 contract.

(3) When a certificate of possession is submitted, the contractor **may** maintain the classified matter for 2 years, unless notified to the contrary by the appropriate Departmental element. The format of the certificate of possession is up to the responsible contracting office. Suggested formats are letter, memorandum, or local form. See Figure II-10 for an example.

e. 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 Departmental element.

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 the DOE under contract # (*contract, subcontract, or other agreement*).

SIGNATURE

TITLE

COMPANY OF CONTRACTOR/SUBCONTRACTOR

DATE

Figure II-9. Example Certificate of Nonpossession 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 item(s) 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 the DOE under contract # (*contract, subcontract, or other agreement*).

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

(*Insert company name*) understands and agrees that:

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 the Atomic Energy Act of 1954, as amended; 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

TITLE

COMPANY OF CONTRACTOR/SUBCONTRACTOR

DATE

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

To accomplish the termination requirements, the CMPC manager **should** coordinate at least the following steps:

(1) Collect, then conduct a 100 percent inventory of, accountable matter. Take appropriate action if any matter is missing.

(2) Check to see whether a moratorium or ongoing litigation restricts his/her actions.

(3) Collect at a central point all non-accountable classified matter. Double-check to ensure that all matter has been returned.

(4) Destroy all copies, except record copies, of all classified documents.

(5) Send all remaining classified *documents* to the site specified by the responsible contracting officer or Departmental element. One large transmission **may** be used as long as a complete list is included.

(6) Send all classified *material* to the site specified by the responsible contracting office or Departmental element.

(7) Once the matter is destroyed or transferred, the Facility Security Officer **must** complete the facility termination procedures described in DOE O 470.1, which includes instructions for completing a certificate of nonpossession.

8. DESTRUCTION.

a. General. Departmental elements and contractors **must** establish procedures for an ongoing review of their classified holdings to reduce their classified inventories 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 General Records Schedules and DOE Records Schedule. When the determination is made to destroy classified matter, the actual destruction **should** occur as soon as possible.

(1) Local destruction procedures **should** be approved and coordinated with the scheduled declassification reviews.

(2) If classified documents are transmitted to an approved offsite location for use during a meeting they should be destroyed at the conclusion of the meeting if no longer needed, including all additional copies created during the meeting. Destroying classified documents at the conclusion of the meeting eliminates the

need to return the classified documents to the originator and the potential for compromise during transmission.

(3) If the Departmental element or organization is 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 Chief Counsel and records management organization.

b. Methods. Classified matter **must** be destroyed beyond recognition to preclude reconstruction. Destruction can be accomplished by burning, shredding, pulping, melting, mutilation, chemical decomposition, or pulverizing. The following additional requirements **must** be satisfied when classified matter is destroyed.

(1) The cognizant DOE security office **must** approve public destruction facilities or any other alternative procedures (e.g., burying or disassembly). If classified matter cannot be destroyed on site, it **must** be destroyed at a public destruction facility by a cleared individual on the same day it is removed from the site.

(2) A record of dispatch is not required unless custody of the matter is released to another cleared contractor or a Government Agency.

(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 Departmental element.

(5) Classified automated information systems media **must** be destroyed by pulverizing, smelting, incinerating, disintegrating, or other appropriate methods.

(6) Certain methods of destruction may require additional considerations and/or approvals before they are used:

(a) Destruction of paper products. Pulpers, shredders, or pulverizers (e.g., hammer mills, choppers, and hybridized disintegration equipment) **should** be used only for the destruction of paper products. Only paper-based products **should** be destroyed by pulping. Water-repellent papers, including Mylar and durable-medium paper substitutes, are not sufficiently destroyed by pulping. Other methods,

such as disintegration, shredding, or burning, **should** be used to destroy these types of papers.

(b) Destruction of high-density-data documents. Classified documents in microform (e.g., microfilm, microfiche, etc.) or similar high-density-data document types **may** be destroyed by burning, chemical decomposition, or other methods as approved by the cognizant DOE security office. The "SEM Micro DoD" shredder also has been approved for these types of documents.

(c) Tapes, diskettes, and cassettes. To ensure that memory is physically destroyed, this matter **may** be sanitized before being destroyed by pulverizing, smelting, incinerating, disintegrating, or other methods as approved by the cognizant DOE security office. Removable and nonremovable hard disks also **may** be destroyed by removing the entire recording surface through sanding or applying acid.

(d) Cylinders and sound recordings. This matter **may** be destroyed by shaving, breaking, tearing, or incinerating.

(e) 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.

(f) Public destruction facilities. Public destruction facilities **may** be used only with the approval of the cognizant DOE security office.

(g) Environmental concerns. Destruction methods such as burning, chemical decomposition, and disintegration may pose environmental hazards. In addition to obtaining advance Departmental element approval to destroy classified matter by such methods, site personnel must determine if approval is also required by Federal and State environmental protection agencies. Consult the responsible environmental management organization to determine the approvals required for these methods of destruction.

(h) Burial. Some sites dispose of classified matter by burying it in specifically identified burial locations. This method requires prior approval of the cognizant DOE security office. Obviously, the primary concern associated with burial is the likelihood of retrieval. When

contemplating burial as a destruction option, site personnel should consider the following:

1 Because paper documents can be destroyed in several effective ways, reserve burial for nonpaper matter only, if possible.

2 Identify a specific location within the burial grounds for classified matter.

3 Access controls **should** be established for this area.

4 Enhance the difficulty of retrieval through some type of "entombment" process (e.g., encasement in concrete).

5 If the classified matter is contaminated, provide additional protection, as well as health and safety measures, as required.

c. Equipment. Classified matter **must** be destroyed by equipment that has been approved by the cognizant security office. The residue output **must** be inspected each time destruction is effected to ensure that established requirements have been met.

(1) Crosscut shredders that produce residue with a particle size not exceeding 1/32 of an inch in width by ½ inch in length **may** be used for destruction of classified paper and nonpaper products, except microfilms.

(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 mills—the perforations **must not** exceed 3/16 inch in diameter.

(b) Choppers and hybridized disintegrators—the perforations **must not** exceed 3/32 inch in diameter.

(4) Specifications. Facilities **should** establish procedures to ensure compliance with the manufacturer's instructions for operating destruction equipment and to ensure continuing effectiveness.

d. Witnesses.

(1) The destruction of classified matter **must** be accomplished by individuals who have appropriate access authorization for the classification of 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. Facilities with only one employee who has the appropriate access authorization **must** contact their Departmental element's security organization for guidance on destruction.

e. Records of Destruction.

(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. Destruction records [i.e., DOE F 5635.9 (see Figure II-11) or a locally approved equivalent] **must** be retained for at least 2 years from the date of destruction (according to the NARA General Records Schedule 18).

When a document is created, its eventual disposition **should** be decided. Organizations **must** decide whether there is a retention requirement for the document and, if so, how long the document is to be retained. The DOE Records Schedule provides guidelines to assist DOE and contractor managers in controlling and managing DOE records. General Records Schedule 18 contains specific references to security-related records.

(2) Disposition of Records. Destruction records **must** be maintained in accordance with both the NARA General Records Schedules and the DOE Records Schedule. General Records Schedule 18 and DOE O 200.1, *Information Management Program,* provide detailed information about records disposition. Organizations also **should** consult the local records management organization for additional assistance and current policy.

f. 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.

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 Manual 471.2-1C, Classified Matter Protection and Control Manual, 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 HAVE 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

Figure II-11. DOE F 5635.9, Record of Destruction (Page 1).

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, S.W., Washington, DC 20585; and to the Office of Management and Budget (0MB), Paperwork Reduction Project (1910-1800), Washington, DC 20503.

Figure II-11. DOE F 5635.9, Record of Destruction (Page 2).

(1) Definition. Non-accountable matter (i.e., any matter classified as Confidential or Secret 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; laser printer cartridges; notes, drafts, and working papers; carbon paper copies; x-rays; floppy disks; imperfect copies of master documents; and any matter in excess of operational needs.

(2) Storage of Classified Scrap. 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 (i.e., envelopes, files, security container drawers, etc.) used as a repository for classified scrap.

(b) Containers **should** be emptied frequently enough to ensure that classified matter is destroyed within 180 days of origination.

NOTE: Non-accountable matter requires neither a witness of destruction nor destruction receipts or certificates.

9. EMERGENCY PROCEDURES. Procedures **must** be developed for safeguarding classified matter in emergency situations.

a. If feasible, classified matter **must** be secured in security containers and, if applicable, the intrusion detection system activated.

b. If the emergency is life threatening, health and safety of personnel **must** take precedence over the need to secure classified matter. Security containers, vaults, and vault-type rooms **must** be inspected on return to the facility to determine whether classified information has been compromised or if any classified matter is missing. Local procedures **should** be developed describing the steps to be followed (i.e., notifications, alternate storage, and protection methods) in case of an emergency.

10. FGI. The requirements provided in this paragraph are additional to other protection and control measures provided in this Manual. These requirements are not applicable to NATO information, which **must** be safeguarded in compliance with the U.S. Security Authority for NATO Instructions. These requirements **may** be modified if necessary or permitted by treaties or agreements, or for other obligations, with the prior written consent of the national security authority of the originating government. Paragraphs 3h(5) and 3w of this chapter also contain FGI requirements.

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. 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 also is required to coordinate with the Joint Atomic Information Exchange Group (JAIEG) before disclosing atomic information. When the information proposed for disclosure contains classified military information, the disclosure **must** be approved in accordance with the National Disclosure Policy.

c. Office of Security and Emergency Operations. The Office of Security and Emergency Operations is responsible for ensuring DOE's compliance with national-level disclosure requirements (such as those of the NDPC and the JAIEG). Prior to implementation, all agreements involving the disclosure of classified information to foreign governments and international agencies **must** be coordinated with the Office of Security and Emergency Operations, 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.

d. Prohibition. 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.

e. 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:

(1) The disclosure **must** be consistent with the foreign policy of the United States toward the receiving government.

(2) 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.

(3) The disclosure **must** be consistent with the national security interests of the United States.

(4) The disclosure **must** be limited to information necessary to the purpose for which disclosure is made.

(5) The receiving government **must** have agreed, either generally or in the particular case, to the following stipulations:

(a) The receiving government **will** not release the information to a third party without the approval of the releasing party.

(b) The receiving government **will** afford the information substantially the same degree of protection afforded the information by the releasing party.

(c) The receiving government **will** use the information *only* for the purpose for which it was given.

(d) If the releasing party indicates that any private rights (such as patents, copyrights, or trade secrets) are involved in the information, the receiving party will acknowledge such rights.

f. Internal Procedures.

(1) Initiation and Coordination. The Office of Arms Control and Nonproliferation **will** initiate and coordinate the necessary procedures to effect the proposed classified information transfers.

(2) Determination of Net Advantage to the United States. The Office of Arms Control and Nonproliferation, in coordination with the General Counsel, the Office of Safeguards and Security, and the responsible program office, **must** determine, as required by paragraph 10e, "that furnishing classified information

will result in a net advantage to the national security of the United States." The Office of Arms Control and Nonproliferation **must** consult with the Department of State and other agencies and departments, as appropriate, in making this determination.

g. Exchange Agreements.

(1) Establishment of Agreement. Prior to developing an exchange agreement, the Office of Security and Emergency Operations **must** confirm the existence of an applicable government-to-government agreement between the United States and the foreign country or international agency involved.

(2) Development of DOE Agreement. The Office of Arms Control and Nonproliferation, in coordination with the Deputy Administrator for Defense Nuclear Nonproliferation and General Counsel (and other program offices as necessary), **must** develop a classified information-exchange agreement for each foreign government or international agency prior to (a) initial transfer of classified documents or material or (b) initial access to material in written or oral form.

(3) Contents. This information-exchange agreement **must** specify the necessary requirements to ensure the security of the transferred documents, material, or information. It **must** be compatible with the terms and conditions of existing government-to-government agreements applicable to the transfer of classified information.

(4) Execution of Agreement. DOE **will** execute the exchange agreement on a finding that the recipient government will provide adequate protection of the information to be furnished.

h. Transfer of Classified Information.

(1) 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.

(2) Review of Documents to be Transferred.

(a) Classified documents or material to be transmitted to foreign governments **must** be forwarded to the Office of Nuclear and National Security Information for classification review. The Office of Security and Emergency Operations **must** ensure that the information

transmitted is within the scope of existing government-to-government agreements and that legal concurrence has been obtained from General Counsel.

(b) If the transfer involves classified information or material produced by or received from another Government agency, the Office of Security and Emergency Operations **must** obtain approval from such agency prior to transmission.

(3) Preparation and Method of Transmission. The preparation, including classification markings and method of transmission of documents, **must** be the same that is prescribed in paragraph 3 for the classification 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 of the Office of Safeguards and Security.

i. Accountability.

(1) Information on oral disclosures, made or contemplated, **must** be contained in memorandums prepared by the Office of Security and Emergency Operations, and maintained by the Office of Safeguards and Security.

(2) Accountability of the information being processed for release **must** be maintained by the Office of Safeguards and Security. The records **must** include the following:

(a) identification of the exact information being released or being processed for release (for documents give document date, title, name(s) of originator(s), and classification);

(b) names and signatures of approving officials;

(c) form in which information is released or is to be released (oral, written, or material);

(d) date of release or contemplated release;

(e) identity of foreign government organization to which, and original individual recipient to whom, release is made or contemplated;

(f) security assurance or security check for each individual recipient;

(g) waivers exercised or requested, where applicable;

(h) statement that the information is based on data originated outside DOE, wherever applicable, and identity of originating organization; and

(i) citation of authority for release by an outside source, if applicable.

j. Handling. Classified information received from foreign governments and international agencies **must** be handled according to those requirements for classified matter set forth in this chapter. Unless specifically identified in transfer agreements, there are no additional handling requirements. In those cases, specific requirements will be associated with the matter in question.

k. Markings.

(1) Classified information from a foreign government **must** be marked in accordance with paragraph 3 of this chapter. Table II-2 lists foreign classification-level markings.

(2) 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."

(3) 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 U.S. origin.

l. Top Secret FGI. The following requirements **must** be implemented for Top Secret FGI:

(1) Top Secret FGI **must** be entered into accountability.

(2) Top Secret FGI **must** be reproduced only with the consent of the originating government.

(3) Destruction of Top Secret FGI **must** be witnessed.

m. Secret FGI. The following requirements **must** be implemented for Secret FGI:

(1) Secret FGI **must** be entered into accountability, if designated by treaties or international agreements.

(2) Secret FGI **must** be reproduced to meet mission requirements, unless specifically prohibited by the originating government.

(3) Destruction of Secret FGI **must** be witnessed.

n. Confidential FGI. No records are required to be maintained for Confidential FGI, unless required by the originator.

o. Confidential FGI—Modified Handling Authorized (C/FGI-MOD). To ensure the protection of other FGI provided in confidence, it **must** be classified under Executive Order 12958. If the foreign protection requirement is lower than the protection required for U.S. Confidential information, the following requirements **must** be met:

(1) Marking C/FGI-MOD. Documents **may** maintain their original foreign markings, if the markings provide immediate recognition that the information requires special protection and control. Otherwise, the first page of the FGI documents **must** be marked as follows:

> This document contains (*insert name of country*) (*insert classification level*) information to be treated as Confidential - Modified Handling Authorized.

If re-marking is impractical, an authorized cover sheet (DOE F 5639.4, Confidential Foreign Government Information Cover Sheet) **may** be used. (See Figure II-12.)

(2) 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.

(3) 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 instructions or by applying the approved cover sheet.

(4) Protection of C/FGI-MOD. C/FGI-MOD matter **must** be protected in the following manner.

DOE F 5639.4
(09-97)

U.S. DEPARTMENT OF ENERGY

C/FGI-MOD

CONFIDENTIAL FOREIGN GOVERNMENT INFORMATION — MODIFIED HANDLING AUTHORIZED —

As defined by Executive Order 12958, Section 1.1(d), "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 enclosed document contains *Foreign Government Information (FGI),* as defined by Executive Order 12958, "Classified National Security Information." This cover sheet shall be applied to FGI for which there is no correlating U.S. Government classification level and marking. This document requires no additional markings.

Access to the enclosed information does not require an access authorization or personnel security clearance. However, access to this information shall only be granted to persons with established, demonstrable need-to-know, and whose official duties require access. This information shall 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 shall be stored in an appropriate security container or cabinet or other location to assure protection against unauthorized disclosure or access by unauthorized personnel.

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

C/FGI-MOD

Derived From: POL-2
Declassify On: X-5

18 U.S.C. SECTION 1001; ACT OF JUNE 26, 1948; 62 STAT. 749; 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 5639.4, Confidential Foreign Government Information Cover Sheet.

(a) Protection in use. Physical control **must** be maintained over any matter marked as containing C/FGI-MOD matter so as to prevent unauthorized access to the information.

(b) Protection in storage. C/FGI-MOD matter **must** be stored to preclude unauthorized disclosure. Such matter **may** be stored with other unclassified matter in unlocked receptacles, such as file cabinets, desks, or bookcases, when Government or Government contractor internal building security is provided during nonduty hours. When such internal building security is not provided, locked rooms or buildings provide adequate after-hours protection. If rooms or buildings are not locked or otherwise controlled, C/FGI-MOD matter **must** be stored in locked receptacles, such as file cabinets, desks, or bookcases.

(5) Reproduction of C/FGI-MOD. 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.

(6) Destruction of C/FGI-MOD. At a minimum, C/FGI-MOD matter **must** be destroyed by using strip cut shredders that result in particles of no more than 1/4-inch-wide strips. Other methods that provide sufficient destruction **may** be approved by the local security office. 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.

(7) Transmission of C/FGI-MOD. 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 standard distribution envelope, such as the U.S. Government Messenger Envelope (SF 65-B) or equivalent, **may** be used to transmit C/FGI-MOD matter.

2 C/FGI-MOD matter **may** be hand-carried, as long as strict control can be maintained at all times.

(c) Over telecommunications circuits. When using telecommunications services—including voice (telephonic, point-to-point), facsimile, narrative message, communications facilities, and radio communications—organizations **must** use 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), then the information **must** be protected by encryption. This **may** be accomplished through DOE public key systems or use of encryption algorithms that comply with all applicable Federal laws, regulations, and standards that address the protection of classified and other Sensitive Unclassified Information (see Chapter 9 of DOE M 200.1-1, "Public Key Cryptography and Key Management"). In emergency situations, facility management 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 interconnected with a public switched-broadcast network (e.g., the Internet) **must** provide precautions (e.g., authentication, file access controls, etc.) to ensure 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 the information is not improperly accessed.

p. Third-Country Transfers. The release or disclosure of FGI to any third-country entity **must** have the prior consent of the originating government, if required by a treaty, agreement, bilateral exchange, or other obligation.

q. FGI Containing Unclassified U.S. Information. Documents containing U.S. unclassified information and FGI **must** be protected as C/FGI-MOD matter.

r. FGI Containing Classified U.S. Information. FGI **may** be enhanced by applying U.S. classified information during the analysis phase of assistance. In these cases, unless there is a current agreement for cooperation (RD of FRD) or appropriate international agreement (NSI) allowing sharing of the specific categories and levels of U.S. classified information, the FGI becomes restricted from return to the originating government or international organization of governments.

11. MATERIAL.

a. Definition. According to the DOE Safeguards and Security Glossary of Terms, classified material is defined as "Chemical compounds, metals, fabricated or processed items, machinery, electronic equipment, and other equipment or any combination thereof containing or revealing classified information."

b. Marking.

(1) Paragraphs 3c(5) and 3d(3) require that classified material have the classification level and category (if RD or FRD) stamped, printed, etched, written, engraved, painted, or affixed 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, first coordinate with the production engineers. War Reserve and Configuration Control requirements mandate strict control over what is done to specific materials—markings **should** not violate these rules. Any alternative markings under consideration **should** be verified as compatible with the material being marked. Such verification will avoid ruining expensive parts by placing unapproved markings on them.

(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 due to the nature of material.

c. Alternatives to Standard Markings.

(1) General. Because material often comes in shapes, sizes, and forms that do *not* facilitate using standard markings, all sites have developed alternatives to the standard markings described in paragraph 3 of this chapter. Site personnel should follow the requirements in this Manual to the maximum extent possible and follow the *intent* of the Manual if compliance with the requirements is impractical. Procedures for all marking systems **must** be approved by the cognizant DOE security office.

(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 (i.e., SRD, CFRD, 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 gloveboxes.

(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.

d. 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 DOE security office.

(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, use the production cycle and production control procedures to facilitate the conduct of all inventories of accountable material.