MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL

1. PURPOSE. This Manual provides detailed requirements to supplement DOE O 471.2, INFORMATION SECURITY PROGRAM, which establishes policy for the protection and control of classified and unclassified information.

2. SUMMARY. This Manual is composed of three 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 protection and 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. Chapter III addresses unaccounted-for matter and compromise of classified information.

3. DEVIATIONS. Deviations to this Manual shall be approved through procedures established in DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM.

4. ASSISTANCE. Questions concerning this Manual should be directed to the Classified Matter Protection and Control Program Manager, at 301-903-4805.

5. IMPLEMENTATION. Most requirements in this directive are the same as those contained in the superseded directives. Implementation Plans for any requirements that cannot be implemented within 6 months of the effective date of this Manual or within existing resources shall be developed by Heads of Field Elements and submitted to the Office of Safeguards and Security.

BY ORDER OF THE SECRETARY OF ENERGY:

ARCHER L. DURHAM
Assistant Secretary for
Human Resources and Administration

TABLE OF CONTENTS

CHAPTER I

PROTECTION AND CONTROL PLANNING

1. SITE-SPECIFIC CHARACTERISTICS. Protection programs shall 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 Policy for the Department of Energy (DOE) Programs and Facilities (U)" shall 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 shall incorporate the applicable requirements established in Chapter II. In addressing the threat to the Department's information assets, emphasis must be placed on security systems that will detect or deter unauthorized disclosure, modification, or loss of availability of classified and sensitive but unclassified information and its unauthorized removal from a site or facility.

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

4. PLANNING.

   a. Site Safeguards and Security Plans. The details of site protection measures shall 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 shall be developed to describe the protection program in place.

5. 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 security interest are commensurate with the security interest's importance or the impact of its loss, destruction, or misuse. Interests whose loss, theft, compromise, and/or unauthorized use will have serious impact on the national security and/or the health and safety of DOE and contractor employees, the public, the environment, or programs shall be given the highest level of protection. For example, use of a weapon of mass destruction by a terrorist(s) could have consequences so grave as to demand the highest attainable standard of security. Protection of other interests shall be graded accordingly. Asset valuation, threat analysis, and vulnerability assessments shall 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 shall 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 risks will be accepted (i.e., that actions cannot be taken to reduce the potential for or consequences of all malevolent events to zero); however, an acceptable level of risk will be determined based on evaluation of a variety of facility-specific goals and considerations. Protection-related plans shall describe, justify, and document the graded protection provided the various safeguards and security interests.

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 October 1994. Departmental Elements are cautioned, however, that the U.S. Security Policy Board has directed that the physical protection requirements in that Manual be reviewed and revised as a matter of priority.

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

   b. Access to classified matter shall be limited to persons who possess appropriate access authorization and who require such access (need-to-know) in the performance of official duties. Controls shall be established to detect and deter unauthorized access to classified matter.

   c. Custodians and authorized users of classified matter are responsible for the protection and control of such matter.

   d. Buildings and rooms containing classified matter shall be afforded the security measures necessary to prevent unauthorized persons from gaining access to classified matter, specifically to include security measures to prevent unauthorized visual and/or aural access.

2. IN USE. Classified matter in use shall be constantly attended by or under the control of a person having the proper access authorization and a need-to-know who is responsible for its protection. Local Departmental and/or contractor safeguard and security authorities may establish written local policy that allows Confidential and/or Secret matter to be left temporarily unattended during normal working hours within a locked room that is within an attended Limited Area, Protected Area, or Exclusion Area. The period of time shall not exceed 2 hours. Unattended within a locked room for up to 2-hour periods in such cases is considered "In Use."

3. MARKING. Within 6 months of the date of this directive, the following requirements shall be fully implemented. Classified matter marked according to previous requirements need not be remarked 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 [nd category if Restricted Data ([RD) or Formerly Restricted Data (FRD)].

      (2) Classification Markings. The term "classification markings" comprises the following elements: classification level, classification category (if RD or FRD), caveats (special markings), classifier information, and originator identification. From this point forward, the term "classification markings" means the markings listed above. Any deviation from the standard classification markings will be stated specifically.

      (3) Other Markings. Markings other than classification markings are date of origin, classification of titles, unique identification numbers (accountable only), destruction date (TOP SECRET only), and portion marking (Originally classified NSI only). These markings are covered later in this chapter.

      (4) Specific examples of markings, including their recommended use, format, and placement, are contained in DOE G 471.2-1, CLASSIFIED MATTER PROTECTION AND CONTROL IMPLEMENTATION GUIDE.

b. Originator Identification. Classified documents shall be marked on the first page to show the name and address of the organization responsible for their preparation and the date of preparation.

c. Classification Level.

(1) The overall classification level of a document shall be marked top and bottom on the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover or last page.

(2) The highest classification level (to include unclassified) of each page shall be marked at the top and bottom of interior pages of classified documents; when individual page marking is not feasible, the overall classification level of the document may be used instead.

(3) These document markings shall be clearly distinguishable from the informational text.

(4) Classified material shall have 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 shall be furnished to recipients.

d. Classification Category.

(1) Documents containing RD or FRD must be marked in the following manner: the overall classification category shall be marked on the outside of the front cover (if any), on the title page (if any), and on the first page. These markings shall be clearly distinguishable from the informational text.

(2) Classified material shall have 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 shall be furnished to recipients.

e. Mixed Levels and Categories. 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. If a matrix is used, the following marking matrix, or one similar in content, will be used in addition to other required markings:

This document contains:

___ Restricted Data at the ____(e.g., CONFIDENTIAL)level.
___ Formerly Restricted Data at the (e.g., TOP SECRET) level.
___ National Security Information at the (e.g., SECRET) ___level.
___ Classified according to: (Guide or Source and Date).

f. Components. When components of a document are to be used separately, each major component shall be marked as a separate document. Components include annexes or appendices, attachments to a letter, and major sections of a report. If an entire major component is unclassified, "UNCLASSIFIED" may 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.

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 may be placed on the top and bottom of the cover (if any), title page (if any), and first page.

h. Portions.

(1) For National Security Information (NSI) classified by an Original Classifier, each section, part, paragraph, or similar portion of a classified document shall 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, and (U) for UNCLASSIFIED shall be used. Classification levels of portions of a document shall be shown by the appropriate classification symbol placed immediately following the portion's letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion. Documents containing derivatively classified NSI are not required to be portion marked.

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

(3) Portions of U.S. documents containing foreign government information shall be marked to reflect the foreign country of origin as well as the appropriate classification level, for example, (U.K.-C) indicating United Kingdom-Confidential, or (FGI) indicating Foreign Government Information.

(4) Portions of U.S. documents containing North Atlantic Treaty Organization information shall indicate NATO or COSMIC, including the appropriate classification level; for example, (NATO-S) or (COSMIC-T.S.).

(5) If portion is exempt from automatic declassification, the exemption category number should be placed immediately following the classification level; for example, (SX2) or (CX8).

i. Subjects and Titles. Except for extraordinary circumstances, unclassified subjects and titles shall be used for classified documents. Subjects or titles shall be marked with the appropriate classification level (and classification category if RD or FRD); for example, (U), for unclassified titles or subjects and, when necessary, (TS), (S), or (C) for classified titles or subjects. The symbols shall be placed immediately following the title or subject.

j. Classifier Information. DOE 5650.2B, IDENTIFICATION OF CLASSIFIED INFORMATION, specifies the classifier information that must be contained on classified matter. The required information is as follows:

(1) Classification Authority (original classification and RD only).

(a) Name or personal identifier of the authorized classifier.

(b) Position title of the authorized classifier.

(2) Justification for Classification.

(a) NSI classification category (original classification only).

(b) Designation of the guide or source document and date (derivative classification only).

(3) Duration of classification (NSI only).

(a) Date. Date of reclassification (if applicable), date of declassification, or exemption category.

(b) Exemptions from automatic declassification at 10 years, if applicable, must be placed on the "Declassify On" line.

(c) Exemptions from automatic declassification at 25 years, if applicable, must be placed on the "Declassify On" line.

(d) Extensions. If the classification is extended, the new declassification date must be added.

k. Top Secret Destruction Date. When upon origination or reproduction it is determined that TOP SECRET matter shall be destroyed at a particular time, the classifier shall note this fact on all copies except record copies.

l. Caveats. In addition to the markings specified above, as appropriate, classified matter shall be marked with caveats as indicated below.

(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, shall 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 may not be reproduced without the specific, written approval of the originator.

(2) Foreign Government Information. The notice "FOREIGN GOVERNMENT INFORMATION" is used on U.S. documents to ensure that information of foreign origin is not declassified prematurely or made accessible to nationals of a third country without the consent of the originator.

(3) North Atlantic Treaty Organization (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.

(b) NATO UNCLASSIFIED (NU). This marking, applied to NATO information that does not require security protection, is handled in accordance with information management procedures.

(c) ATOMAL. The ATOMAL category is either U.S. Restricted Data or Formerly Restricted Data 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 upon 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 and Naval Nuclear Propulsion Information (NOFORN only).

(a) No Foreign Dissemination (NOFORN). This marking indicates that the information contained in the document must not be released to foreign nationals or any parties representing foreign interests, nor to members of the public because this is considered to be tantamount to foreign disclosure.

(b) Originator Controlled (ORCON). This marking indicates that the document bearing the marking is controlled by the originator. Reproduction, extraction of information, or redistribution of such documents require the permission of the originator.

(c) Proprietary Information (PROPIN). This marking indicates that the information contained in the document must not be released in any form without the permission of the originating agency to an individual, organization, or foreign government that has any interests, actual or potential, in competition with the source of the information.

(d) Authorized for Release to Country (REL). This marking applies to classified intelligence that 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).

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

(a) Sigma Category. This marking refers to Restricted Data and Formerly Restricted Data specifically defined in twelve separate categories (1-5 and 9-15) concerning the design, manufacture, or use of atomic weapons or nuclear explosive devices.

(b) Critical Nuclear Weapons Design Information (CNWDI). A Department of Defense marking designating TOP SECRET or SECRET Restricted Data revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munitions, or test device.

(c) Sensitive Use Control Information (SUCI). This marking refers to classified matter containing information (sigmas 14 and 15), the knowledge of which would significantly enhance an adversary's ability to circumvent a weapon's use control features.

m. Re-marking Downgraded/Declassified Matter. Matter marked for automatic downgrading or declassification may be downgraded or declassified and re-marked accordingly. Matter not marked for automatic downgrading or declassification will remain classified until a determination is made by the originating agency.

n. Upgrading Classified Matter. Upon receiving an official upgrade notice, the original classification-level markings should be stricken and replaced with the new classification-level markings. The authority for and date of the upgrading notice should be entered on the first page of the document and all known holders of the document notified.

o. Marking Special Documents. Unless otherwise stated, the standard classification marking requirements remain in effect. The following are nonstandard configurations of the classification markings.

(1) Charts, Maps, Drawings, and Tracings. When such documents are printed on larger than standard (8.5 x 11 inch) sheets, the overall level of the document shall be marked under the legend, title, or scale block. Classification level shall be visible when these types of documents are folded or rolled.

(2) Messages. The overall classification level (and category if RD or FRD) of the message shall 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, downgrading instructions shall be included on the last line of text and may be abbreviated as follows.

DNG/S or C (date or event); or
DECL (date or event).

(3) Microforms.

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

(b) Microfiche and Microfilm. All microforms shall contain markings specified by this chapter (with the exception of classifier, classification guide, and declassification information) on the medium (e.g., microfiche or reel) and its container (e.g., paper sleeve or box).

(c) Microform Document Images. All classification markings shall be marked on the individual documents contained on the microforms.

(4) Motion Picture Films or Video Tapes. At the beginning of a film or videotape, the following information shall 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 videotape, the classification level shall be projected for approximately 3 seconds. The face of the videotape cartridge or the face/side of the film's reel shall be marked with the classification level and category (if RD or FRD).

(5) Photographs. Roll negatives or positives shall be marked at the beginning and end of each strip. Prints and reproductions shall show the classification level and category (if RD or FRD) on the face side of the print. Other classification markings shall 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 shall be protected at the classification level (and category if RD or FRD) of information contained on the media.

(6) Transparencies, Slides, and Sheet-Film.

(a) Classification level and category (if RD or FRD) shall be shown on the image of the first transparency, slide, or sheet film of a series. All other applicable markings specified in this chapter shall 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, classification level.

(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.

(7) Recordings. Magnetic, electronic, or sound recordings shall indicate the overall classification level (and category if RD or FRD) at the beginning and end of the recording.

(8) Classified Information Systems Media. Specific requirements for the handling of classified information system media are addressed in DOE

M 5639.6A-1, MANUAL OF SECURITY REQUIREMENTS FOR THE CLASSIFIED AUTOMATED INFORMATION SYSTEM SECURITY PROGRAM.

(9) Translations. U.S. classified information translated into a foreign language shall be marked as U.S. classified information, and shall show the equivalent foreign government classification.

(10) Radiographs and X-rays. When standard markings are not practical on the radiograph or x-ray, they shall 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.

(11) Training Matter. Unclassified matter used to simulate or demonstrate classified matter for training purposes must be clearly marked to indicate that it is unclassified.

p. File Folders and Other Containers. When not in approved secure storage repositories, file folders and other items containing classified documents shall be marked conspicuously to indicate the highest classification level of any classified matter included.

q. Transmittal Documents. The first page of a transmittal document shall 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 shall be included on transmittal documents when they convey restrictions.

r. 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 need only contain the following markings.

(1) The date created.

(2) The highest classification level (and category if RD or FRD) of any information contained therein.

(3) The annotation "WORKING PAPERS" or "DRAFT" on the cover (if any), the title page (if any), and the first page.

(4) Those prescribed for a finished document of the same classification 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.

s. 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.

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

u. Cover Sheets. The Standard Form (SF) cover sheet shall be applied to all classified documents when removed from a secure storage repository. Contractors may use locally developed cover sheets of the same color and format as the standard forms. SF 703 is the TOP SECRET cover sheet, SF 704 is the SECRET cover sheet, and SF 705 is the CONFIDENTIAL cover sheet. In lieu of standard forms, a National Security Council cover sheet shall

be affixed to each copy of a document containing classified National Security Council information.

4. ACCOUNTABILITY AND CONTROL SYSTEMS.

a. General. Control systems shall be established and used to prevent unauthorized access to classified information. Accountability systems provide a system of procedures that provide an audit trail.

(1) Accountable matter includes TOP SECRET matter; SECRET matter stored outside of a limited area (or higher); and any matter that requires accountability by national, international, or programmatic requirements.

(2) SECRET matter used or processed outside a limited area need not be placed into accountability if the classified matter can be protected in accordance with the requirements of Chapter II, paragraph 1d.

b. Control Stations. Control stations shall be established and used to maintain records and control classified matter (including facsimiles) received by and/or dispatched from facilities. Employees must be designated and trained to operate these control station(s), and the employees shall have access authorizations commensurate with the level of their classified control responsibilities. TOP SECRET Control Officers shall function as control stations for TOP SECRET matter.

c. Top Secret Access Records. An up-to-date record (i.e., DOE F 5635.4, "Top Secret Access Sheet" or a form similar in content) shall be maintained for all persons who are authorized access (including visual or aural access) to TOP SECRET information. The record shall identify the item of TOP SECRET matter, show the name of each individual given access, and show the date (or inclusive dates) of access. For employees whose duties require knowledge of the combination of containers holding TOP SECRET matter, the SF 700 is the only access record that needs to be retained for the combination.

d. Accountability Records. Accountability records are required when accountable matter is originated, reproduced, transmitted, received, destroyed, or changed in classification. Control station operators shall maintain accountability systems for accountable matter. As a minimum, accountability records shall indicate the following information for each accountable item.

(1) Date of the matter.

(2) Brief description of the matter (unclassified if possible).

(3) Unique identification number.

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

(5) Disposition of the matter (for example: destruction, downgrading, declassification, dispatch outside the facility, or incorporation in another accountability record) and the date.

(6) Originator Identification.

(7) Number of copies of documents generated or reproduced.

(8) 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.

(9) Date received, if applicable.

(10) Activity from which the matter was received, if applicable.

e. Inventory. An annual inventory of accountable matter shall 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 shall be submitted in accordance with Chapter III.

f. Records Disposition. Records maintained to control and account for classified matter, including those reflecting receipt, dispatch, and destruction, shall be retained in accordance with the DOE Records Schedule and the National Archives Records Administration's General Records Schedules.

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 shall 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 of the same classification when the working papers 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. Classified Information System Media.

(1) Removable Storage Media. Removable storage media that contains accountable classified information shall be entered into accountability in the same manner as working papers and drafts. Appropriate data regarding the existence of accountable fixed media shall be identified in the security plan and maintained with the system documentation. Accountability is not required for storage media that contains non-accountable classified information.

(2) Files and Documents. Accountability is not required for individual files/documents contained on storage media regardless of the classification level involved.

(3) Top Secret. Contractors must maintain a system identifying the contracting activity, the classified contract, and a general description of the TOP SECRET information contained on the storage media. This requirement may be accomplished through maintaining current back-up copies of the information, generating a directory listing/index of the classified files, or documenting the classified files accessed in the security operation log.

5. REPRODUCTION.

a. General.

(1) Documents may contain markings that limit reproduction without the specific, written approval of the originator.

(2) Departmental Elements and contractors shall establish local controls for the reproduction of classified documents. Reproduction of classified documents shall be limited to the minimum number of copies consistent with operational requirements and any further reproduction limitations shown on the document.

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

(4) Reproduction restrictions shall 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 Chapter III, paragraph 9.

b. Top Secret. Only TOP SECRET Control Officers may reproduce TOP SECRET documents. TOP SECRET matter shall not be reproduced or photographed without written authorization. However, an approved contract that requires generation or reproduction of TOP SECRET matter will satisfy this requirement, and additional authorization will not be required.

c. Secret and Confidential. Unless specifically prohibited, SECRET and CONFIDENTIAL documents may be reproduced without the permission of the originator. Documents shall only be reproduced in the performance of official and contractual duties.

d. Equipment. Classified documents shall be reproduced on equipment specifically designated for such purpose. To the greatest extent possible, these machines shall be located within Limited Areas, Protected Areas, or Exclusion Areas.

e. Mailing Lists. When graphic arts facilities receive standard mailing or distribution lists for the purpose of mailing reproduced classified documents, either the appropriate Departmental Element or the prime contractor is responsible for verifying the need-to-know, facility approval, and protection capability of the intended recipients of the documents. If this requirement and appropriate instructions have been levied on the graphic arts facility in the contract or subcontract, additional verification is not necessary. Any changes in the standard mailing list are also the responsibility of DOE or the prime contractor.

6. RECEIPT AND TRANSMISSION.

a. General. Classified matter may be transmitted only in the performance of official and contractual duties. Unless the transmission is required by the specific terms of the contract or required for performance of the contract, written authorization of the contracting Departmental Element is required prior to contractors transmitting classified matter outside a facility.

b. Receiving. When classified matter is received at a facility, the following controls shall apply.

(1) Classified matter shall be delivered with the inner envelope unopened to personnel designated to receive it at a control station(s) or to the TOP SECRET Control Officer. Procedures shall 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.

(2) The package shall be examined for any evidence of tampering, and the classified contents checked against the receipt (if provided). Evidence of tampering shall be reported promptly to the cognizant DOE security office. If the matter was received through the U.S. Postal System, the appropriate U.S. Postal Inspector shall also be promptly notified. Discrepancies in the contents of a package shall be immediately reported to the sender. If the shipment is in order and includes a receipt, the receipt shall be signed and returned to the sender, and a copy of the receipt maintained with the control station records.

c. Packaging. Classified matter to be transmitted outside a facility shall be double-wrapped (enclosed in opaque inner and outer containers) except as specified below.

(1) When envelopes are used for packaging, the classified information shall be protected from direct contact with the inner envelope. The inner envelope shall be sealed and marked with the receiver's and the sender's classified mailing addresses, the highest classification of the contents, and any appropriate caveats. The outer envelope shall be sealed and marked with the receiver's and the sender's classified mailing addresses. No markings or notations shall be made indicating that the contents are classified.

(2) If the item is of a size, bulk, weight, or nature precluding the use of envelopes for packaging, other containers of sufficient strength and durability shall 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) shall 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 shall be addressed to a classified mailing address, return addressed to a classified mailing address, and marked with the highest classification of the contents and any appropriate caveats. The outer container shall be addressed to a classified mailing 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 shall be marked with the classification of the equipment but the address and return address may be omitted. The outer container shall be addressed to a classified mailing 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 shall 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 (to include TOP SECRET), the briefcase may serve as the outer container. The inner container shall be addressed, return addressed, and marked with the highest classification of the contents and with any appropriate caveats. The briefcase (outer container) must indicate the return classified mailing address and shall contain no markings to indicate that the contents are classified. A briefcase may not serve as the outer container for travel aboard commercial aircraft.

d. Receipts. For all accountable and all SECRET matter, DOE F 5635.3, "Classified Document Receipt," or a receipt comparable in content, shall be used to transmit classified matter outside of facilities. Receipts shall identify the classified contents and the name and address of both

the sending and receiving facilities. Receipts shall not contain classified information. The receipt shall 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.

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

(a) transmission of matter within a facility.

(b) hand-carrying of matter.

(c) transmittal of CONFIDENTIAL matter.

(2) Top Secret. Transmittal of TOP SECRET matter shall be controlled by a continuous receipt system, both inside and outside the facility. DOE F 1540.2, "Courier Receipt," shall be used by the TOP SECRET Control Officer when TOP SECRET matter is transmitted by a courier.

(3) Returning Receipts. The receiver of any classified matter that contains a receipt must complete the receipt and return it to the sender as soon as possible.

(4) Suspense Copy. When a receipt is required, a duplicate copy of the receipt shall 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) shall be established, and follow-up action shall 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 shall be conducted and the possible loss of the matter shall be reported in accordance with DOE O 471.2. Copies of signed receipts for classified matter shall be retained at control stations in accordance with the DOE Records Schedule and the National Archives and Records Administration's General Records Schedules.

e. Classified Mailing Address.

(1) Classified matter shall be addressed only to classified mailing addresses.

(2) Classified mailing addresses must be verified through the Safeguards and Security Information Management System.

(3) Office code letters, numbers, or phrases shall be used in an attention line for internal routing.

(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 facility at which only one cleared employee is assigned, the outer container shall specify the following:

TO BE OPENED BY ADDRESSEE ONLY
POSTMASTER -- DO NOT FORWARD
IF UNDELIVERABLE TO ADDRESSEE,
RETURN TO SENDER

(5) Mail addressed in this manner shall be delivered only to the addressee or to an agent the addressee has authorized in writing to receive such mail. Only personnel having an appropriate access authorization may be designated as agents for the addressee.

f. Within Facilities. Classified matter transmitted within a facility shall be prepared to ensure adequate security protection for the classification involved and the method of transmission. Double-wrapping is not required;

however, in all cases, measures shall be taken to protect against unauthorized disclosure. The matter may be transmitted by:

(1) personnel having an appropriate access authorization for the level and category of classified information involved; or

(2) approved electronic means.

g. Top Secret Outside of Facilities.

(1) Individuals may be authorized to hand-carry TOP SECRET in accordance with Chapter III of this Manual, paragraph 7j.

(2) When authorized by the Director of Safeguards and Security, TOP SECRET may also be transmitted by the Defense Courier Service, or the Department of State Courier System.

(3) TOP SECRET may be transmitted over approved communications networks. See DOE 5300.3D, TELECOMMUNICATIONS: COMMUNICATIONS SECURITY, for secure communications requirements.

(4) Outside the U.S., provided that the means of transportation is under U.S. military control or under U.S. registry, matter may be transmitted in the custody of a cleared individual who is authorized and specifically approved by a responsible DOE authority for safeguards and security. Written authorization from Headquarters, Office of Safeguards and Security, must be obtained prior to hand-carrying TOP SECRET outside of the U.S.

h. Secret Outside of Facilities.

(1) SECRET matter may be transmitted by any method approved for the transmission of TOP SECRET matter. The use of postal services is not permitted for the transmission of SECRET COMSEC material or any classified Communications Security (COMSEC) keying material; see the DOE COMSEC Procedural Guide for approved methods of transmission.

(2) SECRET matter may be transmitted through the following postal services.

(a) U.S. Postal Service registered mail and U.S. Postal Service Express Mail within and between the 50 States, the District of Columbia, and Puerto Rico. The Waiver of Signature and Indemnity Block of the U.S. Postal Service Express Mail label 11-B may not be executed, and the use of external (street side) express mail collection boxes is prohibited.

(b) U.S. registered mail through Army, Navy, or Air Force Postal Service facilities, provided that the approval of Headquarters Office of Safeguards and Security is obtained and information does not pass out of U.S. citizen control or through a foreign postal system. This method may be used in transmitting 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.

(c) 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) Commercial express service organizations may be used to transmit SECRET matter in accordance with the provisions contained in paragraph 7k, below.

i. Confidential Outside of Facilities.

(1) CONFIDENTIAL matter may be transmitted by any method approved for the transmission of SECRET matter. This does not include COMSEC material; see the DOE COMSEC Procedural Guide for approved methods.

(2) CONFIDENTIAL matter may be transmitted by U.S. Postal Service Certified within the 50 States, the District of Columbia, Puerto Rico, and U.S. territories or possessions.

j. Authorized Hand-carriers and Escorts.

(1) Employees having an appropriate access authorization may be designated to hand-carry or escort classified matter. Hand-carrying classified matter for the purpose of a meeting or visit outside a facility shall be authorized 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; and

(f) the classified matter can be appropriately stored upon arrival.

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

(a) Authorized individuals shall have an access authorization commensurate with the level of the information involved and be briefed on 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 shall make prior arrangements for storage of classified matter through the host security office. All classified matter, when not in the possession of authorized individuals, shall be stored only in approved facilities.

(c) A responsible facility official shall brief a hand-carrier who does not routinely act as an authorized individual on the responsibilities to protect classified information.

(d) The authorized individual shall retain the classified matter in his/her possession at all times. Arrangements shall be made in advance of departure for overnight storage at an approved facility that has appropriate storage capability.

(e) When escorting shipments of classified matter via rail, individuals shall travel in an escort car accompanying the shipment, keeping the shipment car(s) under observation. When practicable and time permits, individuals shall detrain at stops to watch the shipment car(s) and check car(s) or container locks and seals. In addition, individuals shall maintain liaison with train crews, other railroad personnel, special police, and law enforcement agencies, as appropriate.

(f) When escorting shipments of classified matter via motor vehicle, individuals shall maintain continuous vigilance for the presence of conditions or situations that might threaten the security of the cargo, and take appropriate action as circumstances might require to avoid interference with the continuous safe passage of the vehicle. In addition, individuals shall check seals and locks at each stop when time permits, and observe vehicles and adjacent areas during stops or layovers.

(g) When escorting shipments of classified matter by means of commercial or military aircraft, individuals shall continuously observe plane and cargo during ground stops and cargo during loading and unloading operations.

(h) Classified material may be handcarried aboard commercial passenger aircraft by cleared employees with the approval of the Facility Security Officer. Cleared employees shall follow the procedures contained in FAA Advisory Circular AC 108-3, "Screening of Persons Carrying U.S. Classified Material."

k. Commercial Express Service Organizations. The use of commercial express delivery service for transmitting classified matter is restricted to emergency situations where the information positively has to be at the receiving facility(ies) on the next working day. Commercial express service shall not be used as a matter of routine or convenience for transmitting classified matter. As a minimum, the sender shall ensure the following conditions are met.

(1) The express service organization has been approved by the Office of Safeguards and Security. Approval by Departmental Elements shall conform to requirements established by the Office of Safeguards and Security, specific to each approved express service organization.

(2) The transmittal address, identified in the Safeguards and Security Information Management System as the Overnight/Classified Common Carrier Address, is used.

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

(4) All packages will be double wrapped before being inserted into the packaging provided by the commercial express service organization.

(5) The properly wrapped package is hand-carried to the express mail dispatch center in sufficient time to allow for dispatch on the same day.

(6) 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.

l. Common Carrier Shipments. The following classes of common carrier services may be utilized upon approval by the cognizant local safeguards and security authority.

(1) Motor carriers in exclusive use that provide locked and sealed van service.

(2) Locked and sealed railroad car, provided the carrier shall furnish a report on request identifying the car location.

(3) Air carriers providing prompt tracking and special signature services.

(4) Commercial messenger services engaged in the intracity/local area delivery (same day delivery only) of classified matter between cleared facilities and to the U.S. Post Office.

(5) Rail, truck, or air without escort, or special protective services, when size and weight together preclude removal without the aid of mechanical devices, and when the containers are securely banded, sealed, and otherwise fastened so as to readily reveal any attempted opening or unauthorized access.

m. Additional Requirements. Shipments of classified matter, including bulk document shipments, are subject to the following conditions, unless more stringent requirements are imposed elsewhere.

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

(2) Seals or other tamper-resistant devices shall be used on shipping vehicles and containers, and be placed in a manner to show evidence of tampering. The type of seal to be used is to be determined by local safeguards and security authority. Seals shall have serial numbers. Seal identification shall be entered on bills of lading or other shipping papers. Seal numbers shall be verified by the consignee upon arrival of a shipment.

(a) Combination padlocks meeting Federal Specification FF-P-110 shall 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 shall 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.

(c) Unescorted shipments by rail or truck (e.g., truckload or carload) shall be made under arrangements with carriers to provide in-transit reports as needed. The carrier shall provide immediate notice concerning any serious delay of the shipment.

(3) Assurances and Notifications.

(a) Carrier must be approved according to DOE O 470.1.

(b) Notification of shipments shall be transmitted to the consignee prior to departure with sufficient time to enable proper handling at the destination. As a minimum, the notification shall 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 shall advise the consignor of any shipment not received within 48 hours after the estimated time of arrival furnished by the consignor or transshipping activities personnel. Upon receipt of such notice, the consignor shall immediately initiate tracing of the shipment.

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

(a) Sufficient personnel shall be tasked for a specific movement assignment to ensure continuous protection of the matter being transported.

(b) Use of rail, truck, air, and other modes of transportation shall be based on protection meeting the requirements outlined in subparagraphs 1, and 2 below.

1 As a minimum, the common carrier or other service shall be required to provide the following security services.

a Surveillance by an authorized carrier employee when the classified matter is outside the vehicle.

b A tracking system that ensures prompt tracing of the shipment while en route.

c When storage is required, classified matter shall be stored in an alarmed or guarded storage area with immediate response by a carrier employee, commercial guard, or police officer.

2 Verification shall be made of the identity and authorization of person(s) who pick up the classified matter.

7. CONTRACT CLOSEOUT/FACILITY TERMINATION.

a. General. Classified matter received or generated in the performance of a classified contract shall be returned to DOE on completion of the contract unless the matter has been declassified, destroyed, or retention is authorized.

b. Contract Completion. Upon completion or termination of a contract, the contractor must submit, to the Contracting Officer, either a certification of nonpossession or a certification of possession. The Contracting Officer shall then transmit the certifications to the cognizant security office.

c. Certification of Nonpossession.

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

(2) When a Departmental Element's facility approval is to be terminated, a certificate of nonpossession must be completed as part of the facility termination process.

d. Certification of Possession.

(1) Requests to retain classified matter shall indicate the benefit to DOE and the intended use of the information. Certifications must specifically identify each piece of TOP SECRET matter and identify SECRET and CONFIDENTIAL matter by subject matter, the type or form, and the quantity of matter.

(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, a copy of the retention notification shall be provided to the Departmental Element or the other Government agency holding the contract. 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 certification of possession is submitted, the contractor may maintain the classified matter for 2 years unless notified to the contrary by the appropriate Departmental Element.

e. Termination of Facility Approval. Notwithstanding the provisions for retention outlined above, if a facility approval is terminated for any reason, classified matter in the facility's possession shall be returned

to DOE or disposed of in accordance with instructions from the Departmental Element.

8. DESTRUCTION.

a. General. Departmental Elements and contractors shall establish procedures for an ongoing review of their classified holdings to reduce their classified inventory to the minimum necessary. Multiple copies, obsolete matter, and classified waste shall be destroyed as soon as practical. Classified matter shall be destroyed in accordance with records disposition schedules, including the National Archives and Records Administration General Records Schedules and DOE Records Schedule.

b. Methods. Classified matter shall 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 Departmental Element must approve public destruction facilities or any other alternative procedures (e.g., burying or disassembly). If classified matter cannot be destroyed at the facility, it shall be destroyed on the same day it is removed from the facility.

(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.

c. Equipment. Classified matter shall be destroyed by equipment that has been approved by the cognizant security office. The residue output shall be inspected each time destruction is effected to ensure that established requirements are 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 non-paper products, except microfilms.

(2) Pulping equipment shall be equipped with security screens with perforations of 1/4 inch or smaller.

(3) Pulverizing equipment shall be outfitted with security screens that meet these specifications.

(a) Hammer mills - the perforations shall not exceed 3/16 inch in diameter.

(b) Choppers and hybridized disintegrators - the perforations shall not exceed 3/32 inch in diameter.

NOTE: When self-processing film or paper is used to photograph or reproduce classified information, all parts of the last exposure shall be removed from the camera and destroyed as classified waste, or the camera shall be protected at the classification level (and category if RD or FRD) of information contained on the media.

d. Witnesses.

(1) The destruction of classified matter shall be accomplished by individuals having appropriate access authorization commensurate to the classification of matter to be destroyed.

(2) The destruction of SECRET or CONFIDENTIAL matter may be accomplished by one individual, no witness is required.

(3) The destruction of TOP SECRET matter shall be witnessed by an appropriately cleared individual other than the person destroying the matter. Facilities with only one employee having the appropriate access authorization shall 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 by using DOE F 5635.9, "Record of Destruction," or a form similar in content, which shall be signed by the individual destroying the matter. An audit trail must be maintained until destruction.

(2) TOP SECRET. When TOP SECRET matter is destroyed, a record of destruction shall be executed indicating the date of destruction and identifying the matter destroyed. The form shall be signed by the individual designated to destroy the matter and the witness to the destruction.

(3) Disposition of Records. Destruction records must be maintained in accordance with the National Archives Records Administration's General Records Schedules and the DOE Records Schedule.

f. Waste. Classified waste shall be destroyed by approved methods as soon as practical. Receptacles utilized to accumulate classified waste shall be clearly marked to indicate its purpose. Pending destruction, classified waste, and receptacles shall be protected as required for the level of classified matter involved.

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

a. If feasible, classified matter shall be secured in security containers and the intrusion detection system activated.

b. If the emergency is life threatening, the health and safety of personnel shall take precedence over the need to secure classified matter. Security containers, vaults, and vault-type rooms shall be inspected on return to the facility to determine whether classified information has been compromised or if any classified matter is missing.

CHAPTER III

UNACCOUNTED-FOR MATTER AND COMPROMISE OF CLASSIFIED INFORMATION

Loss, compromise, or unauthorized disclosure of information and unaccounted-for matter shall be handled according to DOE O 470.1. In addition, the following requirements apply.

1. DISCOVERY. Any person who determines that classified matter has been or may have been lost or compromised or is otherwise unaccounted-for shall take immediate action to preclude any further or potential compromises and immediately report this information to the facility security officer.

2. INSPECTION. Upon determining or learning that classified matter may be lost or unaccounted-for, an inspection shall be completed within 48 hours.

   a. If the matter is found or otherwise accounted for, the inspection will be discontinued.

   b. If Secret or Confidential matter is unaccounted for, the cognizant DOE safeguards and security organization shall be notified within 24 hours following the completion of the inspection. Notifications must also be made in accordance with DOE O 232.1.

   c. If Sigma 1 or Sigma 2 Weapon Data matter is unaccounted for, the Office of Safeguards and Security, the appropriate Secretarial Officer, and the Office of Military Applications, through the cognizant DOE safeguards and security organization, shall be notified within 24 hours following the completion of the inspection.

   d. If Top Secret matter, classified matter of another agency, or classified matter of a foreign government is unaccounted for, the Office of Safeguards and Security and the appropriate Secretarial Officer, through the cognizant DOE safeguards and security organization, shall be notified within 24 hours following the completion of the inspection. Documents related to the Joint Atomic Information Exchange Group shall also be reported to the Deputy Assistant Secretary for Military Application and Stockpile Support, who will ensure appropriate reporting to the Joint Atomic Information Exchange Group.

3. INQUIRY.

   a. When inspection efforts fail to reconcile unaccounted for matter, and for all potential compromises, the appointed Inquiry Official shall initiate an inquiry. The cognizant DOE safeguards and security organization shall advise the Office of Safeguards and Security of the initiation of an inquiry. As a minimum the inquiry shall accomplish the following.

      (1) Obtain signed statements by individuals who may have knowledge regarding the circumstances.

      (2) Complete DOE F 5635.11, "Reporting Unaccounted for Documents" or a form similar in content when matter is unaccounted-for.

      (3) Assess the potential for compromise; if results of the inquiry indicate that a compromise has occurred or may have occurred, notify the cognizant Secretarial Officer.

      (4) When an inquiry establishes credible information that a violation of law may have occurred, the Department of Justice Eleven-point Criteria shall be completed. A positive response must be provided to all eleven points for the Department of Justice to initiate a formal investigation. All documentation and appropriate information must be provided to support affirmative responses to the following interrogatories.

(a) Could the date and identity of the article or articles disclosing the classified information be provided?

(b) Could specific statements in the article that are considered classified be identified? Was the data properly classified?

(c) Is the classified data that was disclosed accurate? If so, provide the name of the person competent to testify concerning the accuracy.

(d) Did the data come from a specific document and, if so, what is the origin of the document and the name of an individual(s) responsible for the security of the classified data disclosed?

(e) Could the extent of official dissemination of the data be determined?

(f) Has it been determined that the data has not been officially released in the past?

(g) Has it been determined that prior clearance for publication or release of the information was not granted by proper authorities?

(h) Does review reveal that educated speculation on the matter cannot be made from material, background data, or portions thereof that have been published officially or have previously appeared in the press?

(i) Could the data be made available for the purpose of prosecution? If so, include the name of the person competent to testify concerning the classification.

(j) Has it been determined that declassification had not been accomplished prior to the publication or release of the data?

(k) Will disclosure of the classified data have an adverse impact on the national defense?

b. A written inquiry report shall be completed, with supporting statements/documentation, and forwarded to the Office of Safeguards and Security and the responsible Secretarial Officer through the cognizant DOE safeguards and security organization through 5000.3B. When the possible compromise involves information or matter from another Government agency or foreign government, the Office of Security Affairs shall ensure the other agency or government is informed of the results of the inquiry and subsequent actions.

c. Upon completion of the inquiry, the cognizant DOE safeguards and security organization shall ensure:

(1) the party or parties responsible for compromise of the classified information are identified, and as appropriate, infractions assigned to individuals and disciplinary actions taken;

(2) protection and control and other security measures are in place; and

(3) corrective actions are taken to preclude recurrence of conditions or activities that allowed or contributed to the compromise of classified information.

4. DAMAGE ASSESSMENTS.

a. Purpose. Damage assessments to assess potential damage to national security are required by 32 CFR, Chapter XX, Part 2000, "National Security Information," Section 2001.47, "Loss or Possible Compromise." Damage assessments are used by responsible managers to determine future courses

of action within the program and by security personnel for evaluating possible countermeasures and cover actions to limit potential damage.

b. When Required. When the inquiries disclose evidence that information may have been compromised and the compromise can reasonably be expected to cause damage to the national security, a damage assessment shall be conducted. Compromises may occur through espionage, unauthorized disclosures to the press or other members of the public, loss of classified information, unaccounted for classified matters, or through various other circumstances. Both circumstances of the loss and sensitivity of the information must be considered in determining when a damage assessment is required.

c. Conduct of Damage Assessment. The Secretarial Officer with programmatic responsibility for the compromised information will appoint a DOE employee responsible for conducting the damage assessment and appoint an assessment team consisting of an authorized classifier and appropriate technical experts (e.g., weapons design, nuclear policy, material production communications, intelligence, etc.) to assist in assessment of the value of the compromised information to foreign governments or hostile organizations.

d. Procedures. The following procedures shall be followed for all DOE damage assessments.

(1) The originator of the compromised information shall provide the cognizant DOE safeguards and security organization with a copy of the compromised information (including a copy of the matter, if appropriate) and rationale/justification for the assigned classification with reference to appropriate classification guides.

(2) The originator shall immediately notify all known holders of the matter of the compromise.

(3) The team performing the damage assessment shall prepare a draft assessment and coordinate it with the originator.

(4) The damage assessment will then be approved by the Secretarial Officer with programmatic oversight of the information and submitted to the Office of Security Affairs.

(5) The assessment team will provide any additional assessment effort and supporting documentation needed by the Office of Safeguards and Security to complete any required DOE action.

e. Content. Damage assessments reports, as a minimum, contain the following.

(1) Identification of the source, date, and circumstances of the compromise.

(2) Classification of the specific information lost.

(3) Description of the specific information lost.

(4) An analysis and statement of the known or probable damage to the national security that has resulted or may result.

(5) An assessment of the possible advantage to foreign powers resulting from the compromise.

(6) An assessment of whether classification of the information should be continued without change; specific information or parts thereof that shall be modified to minimize or nullify the effects of the reported compromise and the classification retained; and whether downgrading, declassification, or upgrading is warranted and, if so, confirmation of prompt notification to holders of any change.

(7) An assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise.

(8) An assessment of other appropriate corrective, administrative, disciplinary, or legal actions.

f. Coordination. Whenever an action is contemplated against any person believed responsible for the compromise of classified information, damage assessments shall be coordinated with the Office of the General Counsel.

g. Combining Similar Documents. Damage assessments may be completed for a group of unaccounted for classified matter discovered during inventory whenever grouping is a logical method of meeting this requirement. A logical grouping includes a situation when multiple matters requiring a damage assessment are related to a programmatic area and would result in similar damage to the national security or advantage to foreign powers.

h. Outside Agency Information. Compromise of an outside agency's classified information shall be reported to the originating agency by the Office of Security Affairs. The report to the originating agency must include all data pertinent to the compromise to assist in their conduct of a damage assessment.

i. Joint Damage Assessments. When a compromise involves another government agency's information, the following conditions apply.

(1) The other agency has the inherent responsibility to conduct the damage assessment on their information that was lost/compromised.

(2) Whenever a compromise involves the classified information of DOE and another agency, and if more than one damage assessment is performed, the Departmental Element responsible for the DOE damage assessment shall provide, through the Office of Security Affairs, the findings to the other agency.

(3) When a joint assessment is to be made, the Office of Security Affairs will coordinate assignment of responsibility between DOE and the other agency.

(4) Whenever a compromise of DOE classified information is the result of actions taken by foreign nationals, by foreign government officials, or by U.S. nationals in the employ of international organizations, the Office of Security Affairs shall ensure, through appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained.

(5) Whenever a compromise of Sensitive Compartmented Information has occurred, the Director, Office of Energy Intelligence, shall consult with the designated representative of the Director of Central Intelligence and other appropriate officials with responsibility for the information involved.

5. NOTIFICATION TO INFORMATION SECURITY OVERSIGHT OFFICE. On receiving written confirmation from a Departmental Element of an unauthorized disclosure of, or access to, National Security Information by a DOE employee, DOE contractor, or consultant, the Office of Safeguards and Security shall notify the Information Security Oversight Office of the details. Such notification shall be given immediately when the disclosure results from systematic problems. Otherwise, semiannual reports of unauthorized disclosures shall be made.

6 RECORDS RETENTION. Records of all actions pertaining to unaccounted for/compromised matter or compromises of classified information must be maintained by the facility security officer and the cognizant Departmental Element safeguards and security organization. Records shall be destroyed 5 years after the close of all associated actions. These records will not be sent to Federal Records Centers.