DOE M 471.2-1B

This Manual has been cancelled by DOE M 471.2-1C, dated 4-17-01, except Chapter III paragraphs 1 and 2 and Chapter IV. Chapter IV was cancelled by DOE O 471.4, *Incidents of Security Concern,* dated 3-17-04.

1-6-99

CLASSIFIED MATTER PROTECTION AND CONTROL MANUAL

U.S. DEPARTMENT OF ENERGY
Office of Security Affairs
Office of Safeguards and Security

Distribution:
All Departmental Elements

Initiated By:
Office of Safeguards and Security

CLASSIFIED MATTER PROTECTION AND CONTROL MANUAL

1. PURPOSE. This Manual provides detailed requirements for the protection and control of classified matter which supplement DOE O 471.2A, INFORMATION SECURITY PROGRAM.

2. CANCELLATION. This Manual cancels DOE Manual 471.2-1A, MANUAL FOR CLASSIFIED MATTER PROTECTION AND CONTROL, dated 1-9-98.

3. APPLICABILITY.

   a. General. This Manual applies to Departmental Elements with access to classified matter.

   b. Application to Contracts. This Manual applies to contractors with access to classified matter. Contractor requirements are listed in the Contractor Requirements Document, Attachment 1.

4. USAGE. This Manual is composed of four 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. Chapter III provides physical protection requirements for classified matter in storage. Chapter IV addresses classified information that has been or may have been lost, potentially compromised, or disclosed to an unauthorized person.

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

6. REFERENCE. Terms used in the Manual are defined in the "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, at 301-903-4805.

8. IMPLEMENTATION. Except for Chapter III, most requirements in this directive are the same as those contained in DOE M 471.2-1A. Implementation plans for any new 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:

RICHARD FARRELL
DIRECTOR OF MANAGEMENT
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 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 this manual. 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 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 for classified matter 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. TRAINING. Personnel whose responsibilities include the generation, handling/use, storage, reproduction, transmission, and/or destruction of classified matter shall receive appropriate training to ensure such matter is not lost or compromised. Personnel responsible for conducting official inquiries into incidents where classified matter is lost, compromised, or potentially compromised shall receive training necessary to perform this duty.

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 are commensurate with its 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, information which would assist an adversary in the development of a nuclear weapon, or

information that would assist an adversary 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 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 January 1995 and its supplement of February 1995.

   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. The originator of matter that is prepared in a subject area that may be classified shall ensure the matter is reviewed for classification by an Original or Derivative Classifier. While the matter is pending classification review it shall be protected at the highest potential classification level and category.

   d. 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 shall be submitted in accordance with Chapter IV.

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

   f. 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 access.

   g. While most of the requirements of this Chapter apply to Foreign Government Information (FGI), a separate paragraph has been established to facilitate the identification of requirements specific to this information.

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

2. IN USE. Classified matter in use shall be constantly attended by or under the control of a person possessing the proper access authorization and a need-to-know. Local Departmental and/or contractor 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 shall not exceed 2 hours. Locks shall

be uniquely coded or keyed, and appropriate control measures implemented to mitigate the risk of unauthorized disclosure. Facilities shall describe the implementation of these protection measures in facility security plans.

3. MARKING. 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 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.

      (2) Markings. The following elements that are common to all classified documents include: 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. Any deviation from these markings will be specifically stated.

      (3) Additional Guidance. 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 (i.e., TOP SECRET, SECRET, or CONFIDENTIAL) of a document shall 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.

      (2) 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.

      (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) The overall category (if RD or FRD) of a document shall be marked on the cover page (if any), title page (if any), and first page of text as follows:

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 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 shall be clearly distinguishable from the informational text.

(3) Classified material (if RD or FRD) 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.

(4) If significant cost and extensive reprogramming of automated information systems are required to implement this requirement, facilities may delay implementation until January 9, 2003, as long as documents generated from the automated information system remain on-site and have a limited life expectancy.

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, in addition to other required markings, will be placed on the cover page (if any), title page (if any), and first page of text:

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 By: (Name and Title): _____.

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 front cover (if any), title page (if any), and first page.

(3) Unclassified sensitive information shall not be marked in a manner that would be confused with markings specified in this Manual for classified information (e.g., CONFIDENTIAL, etc.)

h. Portions.

(1) For National Security Information (NSI), each section, part, paragraph, graphic, figure, or similar portion of any such document dated after 4/1/97 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, (U) for UNCLASSIFIED, (UCNI) for Unclassified Controlled Nuclear Information and (OUO) for Official Use Only 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.

(2) Page changes to NSI documents dated after 4/1/97, shall be portion marked.

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

(4) Portion markings shall include caveats (as applicable).

(5) 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. Foreign Government Information (FGI) shall be indicated in lieu of the country of origin if the country cannot be associated with the information.

(6) 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-TS).

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, category (if RD or FRD) and any caveats (as applicable). The symbols (e.g., U, CRD, S/ORCON) shall be placed immediately following the title or subject.

j. Classifier Markings. Classifier markings shall be applied as follows:

(1) Original Classification (NSI only).

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

1 Name or personal identifier of the original classifier.

2 Position title of the original classifier.

(b) NSI classification category (i.e., "Reason")

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

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

2 Event. A specific event occurring 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).

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 shall 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 shall be revised to include the date of the reclassification, the new declassification date, and the person authorizing the reclassification.

(2) Derivatively Classified NSI.

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

1 Name or personal identifier of the derivative classifier.

2 Position title of the derivative classifier.

(b) Designation of the guidance or source document(s) and date of such documents.

(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).

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 shall 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 shall be revised to include the date of the reclassification, the new declassification date, and the person authorizing the reclassification.

(3) RD and FRD.

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

1 Name or personal identifier of the derivative classifier.

2 Position title of the derivative classifier.

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

k. Caveats. Classified matter shall be marked with caveats, such as those indicated below, when required by DOE directive or national policy.

(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. Marking, protection and control requirements for Foreign Government Information are contained in paragraph 10.

(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. NATO classified information shall 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. 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.

(a) No Foreign Dissemination (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) 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 TO). This marking applies to intelligence information 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 markings are 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.

(6) Naval Nuclear Propulsion Information (NNPI). Classified and sensitive unclassified NNPI is designated:

"NOFORN This document is subject to special export controls and each transmittal to foreign governments or foreign nationals may be made only with the prior approval of the U.S. DOE."

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

m. Remarking Automatically Declassified Matter. Matter marked for automatic declassification may be declassified and re-marked accordingly upon the date or event

identified for declassification. Matter not marked for automatic declassification will remain classified until a determination is made by the originating agency.

n. 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 x 11 inch) sheets, the overall level and category (if RD or FRD) of the document shall be marked under the legend, title, or scale block. Classification level and category (if RD or FRD) shall 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.

(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, declassification instructions shall be included on the last line of text and may be abbreviated as DECL (date, exemption, 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).

(c) Microform Document Images. All common 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 video tape, 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 video tape, the classification level shall be projected for approximately 3 seconds. The face of the video tape 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 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 highest classification level and category of information contained on the media.

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

(a) The overall classification level, category (if RD or FRD), and any caveats 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, 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 shall be regarded as an individual portion, and does not require further portion marking.

(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. The face of the recording medium shall be marked with the classification level and category (if RD and FRD.)

(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.

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

p. 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.

q. 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 need only contain the following markings.

(1) The date created.

(2) The highest potential overall classification level of the draft or work paper shall be marked 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 top and bottom with the highest classification level of that page (to include unclassified) or the overall classification of the document.

(3) The overall category (if RD or FRD) of the draft or working paper shall be marked on the cover page (if any), or title page (if any), or first page of text.

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

(5) Any applicable caveats or special markings should be annotated on the cover page (if any), title page (if any), and the first page of text.

(6) Markings prescribed for a finished document shall 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.

r. 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.

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 Government Agency and Foreign Government Documents Not Conforming to DOE Requirements. Documents received from other government agencies and foreign

governments not 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).

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

4. CONTROL SYSTEMS AND ACCOUNTABILITY.

a. General. Control systems shall be established and used to prevent unauthorized access to or unauthorized removal of classified information. Accountability systems shall provide a system of procedures that provide an audit trail. Accountable matter includes TOP SECRET or SECRET matter stored outside of a Limited Area (or higher); and any matter that requires accountability by national, international, or programmatic requirements.

b. Control Stations. Control stations shall 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 station(s), and the employees shall have access authorizations commensurate with the level of their classified control responsibilities.

c. 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 and the disposition of each copy.

(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.

d. 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 IV.

e. 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.

f. 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 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 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.

g. Classified Information System Media.

(1) Removable Storage Media. Removable storage media that contains accountable classified information shall be entered into accountability. 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 nonaccountable classified information.

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

5. REPRODUCTION.

a. General.

(1) Classified documents may be reproduced without approval of the originator, except where documents 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) Reproduction shall be accomplished by authorized persons knowledgeable of 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 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 II, paragraph 8.

b. Equipment. Classified documents shall 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 shall be located within Limited Areas, Protected Areas, or Exclusion Areas. Technology that prevents, discourages, or detects the unauthorized reproduction of classified documents is encouraged.

6. RECEIPT AND TRANSMISSION.

a. General. Classified matter may 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, written authorization of the contracting Departmental Element is required prior to contractors transmitting classified matter outside of the 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). 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 safeguards and 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 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 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 address, return addressed to a classified address, and marked with the overall level and category (if RD or FRD) of the contents and any appropriate caveats. The outer container shall 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 shall 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 shall 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 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, the briefcase may serve as the outer container. The inner container shall 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 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 TOP SECRET and 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) Facsimile Transmission. Individuals transmitting classified information via facsimile systems shall confirm receipt (written or verbal) with the intended recipient.

(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 used, 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 this Manual 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 Addresses.

(1) Classified matter shall 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 the Safeguards and Security Information Management System and are valid for 30 days from the date of validation.

(3) Office code letters, numbers, or phrases shall 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 shall 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 (4) above 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 (except as noted); 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

(1) approved electronic means.

g. TOP SECRET Outside of Facilities.

(1) TOP SECRET may be transmitted by the Defense Courier Service or the Department of State Courier System.

(2) TOP SECRET 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 in accordance with Chapter II, paragraph 6.j.

h. SECRET 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 may be transmitted via 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 the DOE M 200.1-1, TELECOMMUNICATIONS SECURITY MANUAL for approved methods of transmission.

(b) 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.

(c) 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.

(d) 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 6.k., below.

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

i. CONFIDENTIAL 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.

(3) The U.S. Postal Service is not permitted for the transmission of COMSEC material or COMSEC keying material; see DOE M 200.1-1, TELECOMMUNICATION SECURITY MANUAL for approval methods of transmission.

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

(1) The cognizant Facility Security Officer, as identified on DOE F 5634. 3 or his/her designee, shall be notified whenever classified matter is to be hand carried outside of the facility to ensure appropriate protection measures are implemented. Approval of employees to hand-carry or escort classified matter outside of a facility will be provided by the designated person/organization 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 of the destination area) have been developed and approved by the cognizant DOE security office.

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

(a) Individuals hand-carrying classified matter shall have an access authorization 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 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 DOE approved facilities, or as specified in approved contingency plans.

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

(3) Classified matter may be hand-carried outside the U.S., provided the following conditions are met:

(a) The traveler must possess appropriate access authorization and diplomatic passport;

(b) Written authorization from the Director, Headquarters, Office of Safeguards and Security.

(4) 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. In cases where 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" shall be followed.

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.

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

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

(4) All packages are 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 or picked-up from a Control Station 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 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 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 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) Whenever practicable, 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.

(3) Assurances and Notifications.

(a) Carrier must be have a facility clearance in accordance with DOE O 470.1, including obtaining a favorable Foreign Ownership, Control, and Influence (FOCI) determination.

(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 24 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 with appropriate access authorization shall be tasked for a specific movement assignment to ensure continuous protection of the matter being transported.

(b) As a minimum, the common carrier service shall 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.

3 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.

(c) When shipments are transported by rail, personnel escorting the shipment shall travel in an escort car accompanying the shipment, keeping the shipment car(s) under observation. When practicable and time permits, personnel escorting the shipment shall perform checks of the car(s), container locks, and/or tamper indicating devices. Liaison 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 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 require to avoid interference with the continuous safe passage of the vehicle. During stops or layovers, personnel escorting the shipment shall check tamper indicating devices and locks.

(e) 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 certificate of nonpossession or a certificate of possession. The Contracting Officer shall 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 shall 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.

d. Certificate of Possession.

(1) Requests to retain classified matter shall 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, 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 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.

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 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 on site , it shall be destroyed at a public destruction facility 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.

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 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 non-accountable classified matter may be accomplished by one individual, no witness is required.

(3) The destruction of accountable classified 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 and the witness. An audit trail must be maintained until destruction.

(2) 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, if applicable, 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.

10. FOREIGN GOVERNMENT INFORMATION

a. General.

(1) Foreign government information is safeguarded in order 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 adequate to achieve equivalency, standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. CONFIDENTIAL information, including allowing access to individual with a need-to-know who have not otherwise been cleared for access to classified information. A matrix of US equivalent classification levels is contained in DOE Guide 471.2-1, CLASSIFIED MATTER PROTECTION AND CONTROL IMPLEMENTATION GUIDE.

(2) The front page of documents that contain foreign government information shall include the marking, "This document contains (indicate country of origin) information." If the identify of the specific government must be concealed, the document shall be marked, "This document contains foreign government information."

(3) In cases where the identity of the specific government must be concealed, a separate record that identifies the foreign government shall be maintained in order to facilitate subsequent declassification actions. When classified records are transferred to the National Archives and Records Administration for storage or archival purposes, the accompanying documentation shall at a minimum, identify the boxes that contain foreign government information. If the fact that information is foreign government information must be concealed, the markings described in this paragraph shall not be used and the document shall be marked as if it were wholly of U.S. origin.

(4) 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. NATO classified information shall be safeguarded in compliance with the U.S. Security Authority for NATO Instructions.

(5) The requirements provided in this paragraph 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.

(6) The following paragraphs contain additional requirements pertaining to FGI:

(a) Chapter II., paragraph 3.h.(5)
(b) Chapter II., paragraph 3.t.

b. TOP SECRET. The following requirements will be implemented for TOP SECRET FGI:

(1) Entered into accountability.

(2) Reproduced only with the consent of the originating government.

(3) Destruction will be witnessed.

c. SECRET. The following requirements will be implemented for SECRET FGI:

(1) Entered into accountability.

(2) Reproduced to meet mission requirements, unless specifically prohibited by the originating government.

d. CONFIDENTIAL. No records are required to be maintained for CONFIDENTIAL FGI, unless required by the originator.

e. CONFIDENTIAL FGI - Modified Handling Required (C/FGI-Mod). To assure the protection of other foreign government information provided in confidence, it must be classified under E.O. 12958. If the foreign protection requirement is lower than the protection required for U.S. CONFIDENTIAL information, the following requirements shall be met:

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

"This document contains (insert name of country) (insert classification level) information to be treated as CONFIDENTIAL - Modified Handling Authorized"

If remarking is impractical, an authorized cover sheet (DOE F 5639.4) may be used.

(2) Need-To-Know. Access to C/FGI-MOD does not require DOE access authorization. However, such documents shall only be provided 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 shall be notified of applicable handling instructions. This may be accomplished by a briefing, written instructions or by applying the approved cover sheet.

(4) Protection. C/FGI-MOD will be protected in the following manner:

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

(b) Protection in Storage. C/FGI-MOD matter shall be stored to preclude unauthorized disclosure. Storage of such matter with other unclassified matter in unlocked receptacles, such as file cabinets, desks, or bookcases, is adequate

when Government or Government-contractor internal building security is provided during non-duty 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 shall be stored in locked receptacles, such as file cabinets, desks, or bookcases.

(5) Reproduction. Matter marked as containing C/FGI-MOD may be reproduced without permission of the originator to the minimum extent necessary consistent with the need 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 with all paper paths checked for C/FGI-MOD material. Excess paper containing C/FGI-MOD shall be destroyed as described below.

(6) Destruction. 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 ways providing sufficient destruction may be approved by the local security office. Note that the decision to dispose of any DOE matter, whether or not it contains C/FGI-MOD, must be consistent with the policies and procedures for records disposition.

(7) Transmission. Transmission shall be by means to preclude unauthorized disclosure or dissemination.

(a) Outside a Facility.

1 Matter marked as containing C/FGI-MOD shall be packaged in a single, opaque envelope or wrapping.

2 Any of the following U.S. mail methods may be used: U.S. First Class, Express, Certified, or Registered Mail may be used.

3 Any commercial carrier.

4 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 (Standard Form No. 65-B) or equivalent, may be used.

2 Matter may be hand-carried as long as strict control can be maintained at all times.

(c) Over Telecommunications Circuits. The use of telecommunications services, including voice (telephonic, point-to-point), facsimile, narrative message, communications facilities and radio communications, must consider and use the most security readily available for the transmission of C/FGI-MOD over this form of media. These considerations include, but may not be limited to, physical, personnel, administrative, and communications protective features and any other supplemental controls established to provide an acceptable level of protection for C/FGI-MOD. These protective features must deter access to C/FGI-MOD by unauthorized individuals and restrict public releasability.

If C/FGI-MOD is transmitted over public switched broadcast communications paths (e.g., Internet) then the information must be protected by encryption. In emergency situations, facility management may make a determination to waive encryption requirements.

(d) Automated Information Systems (AIS). The AIS or AIS network must ensure that only personnel authorized access to C/FGI-MOD can access that information. For instance, networks interconnected with a public switched-broadcast network - like Internet, must provide provisions (e.g., authentication, file access controls, etc.) to ensure that C/FGI-MOD is protected against unauthorized access. C/FGI-MOD being transmitted over broadcast networks like the Internet, where unauthorized access is possible, must provide protection (e.g., encryption) to ensure that the information is not improperly accessed.

f. Third-country Transfers. The release or disclosure of foreign government information 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.

g. FGI Containing Unclassified U.S. Information. Documents containing U.S. unclassified information and FGI require protection as C/FGI-MOD.

h. 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 or treaty allowing the 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.

CHAPTER III

PHYSICAL PROTECTION

1. GENERAL REQUIREMENTS. The following general requirements apply to the protection of classified matter.

   a. The protection of classified SNM shall be in accordance with DOE M 5632.1C-1, Chapter II, if the SNM categories and attractiveness levels dictate more stringent requirements; otherwise the provisions of this chapter apply.

   b. Classified information, regardless of its form, shall be afforded a level of protection against loss or compromise commensurate with its level of classification.

   c. When possible, classified matter shall be processed, handled, and stored in security areas providing control measures equal to or greater than those present in Limited Areas. When Top Secret or Secret matter is not processed, handled, and/or stored within Limited Areas or above, it shall be maintained in an accountability system as required in Chapter II of this Manual.

   d. Facilities, buildings, rooms, structures, etc., shall be afforded the protection measures necessary to prevent unauthorized persons from gaining access to classified matter.

      (1) Measures shall be in place to prevent persons from having visual access to classified information.

      (2) Technical Surveillance Countermeasure requirements will be followed as required by the TSCM Procedural Manual.

   e. Sensitive Compartmented Information Facilities and Special Access Program Facilities shall be afforded physical protection in accordance with the Director of Central Intelligence Directive 1/21.

2. STORAGE REQUIREMENTS. The following storage requirements apply to classified matter.

   a. Restrictions on Use of Secure Storage Repositories.

      (1) Funds, firearms, medical items, controlled substances, precious metals, or other items susceptible to theft shall not be stored in the same secure storage repository used to store classified matter.

      (2) Secure storage repositories shall not bear any external classification or other type markings that would indicate the level of classified matter authorized to be stored within the container. For identification purposes, each security container shall externally bear a uniquely assigned number.

b. Security containers required for the storage of classified matter shall conform to the GSA standards and specifications and applicable requirements of DOE M 5632.1C-1, Chapter IX. Classified matter that is not under the personal control of an authorized person shall be stored as prescribed below.

NOTE: Inspections by the protective force shall consist of examination of the exposed surfaces of the container, vault, vault-type-room and steel filing cabinets to determine if there has been any forced entry and to ensure that the container is locked.

(1) Top Secret Matter. Top Secret matter may be stored in one of the following ways:

(a) In a locked, General Services Administration (GSA)-approved security container with one of the following supplemental controls:

1 Under intrusion detection alarm protection with protective force response within 15 minutes of annunciation of the alarm.

2 Protective force, with inspections on a 2-hour basis.

3 Security container equipped with a lock meeting Federal Specification FF-L-2740, only if the container is located in a Limited, Exclusion, Protected, or Material Access Area.

4 Within a Limited, Exclusion, Protected, or Material Access Area random protective force patrols at least once every 8 hours during nonworking hours. Inspect at least 25 percent of the containers once every 24 hours at facilities with large numbers of security containers.

(b) In a vault meeting the criteria established in DOE M 5632.1C-1 and approved by the cognizant DOE element. The vault shall be equipped with intrusion detection protection with protective force response within 15 minutes of alarm annunciation.

(c) In a vault-type room meeting the criteria established in DOE M 5632.1C-1 and approved by the cognizant DOE element. The vault-type-room shall be under intrusion detection alarm protection with protective force response within 15 minutes of alarm annunciation. The vault-type room shall be located within a Limited, Exclusion, Protected, or Material Access Area.

(d) In a vault-type room meeting the criteria established in DOE M 5632.1C-1 and approved by the cognizant DOE element. If located outside of a Limited, Exclusion, Protected, or Material Access Area, the vault-type-room shall be under intrusion detection alarm protection with protective force response within 5 minutes of alarm annunciation.

(2) Secret Matter. Secret matter shall be stored in a manner authorized for Top Secret matter or in one of the following ways:

(a) In a locked GSA-approved security container.

(b) In a vault meeting the criteria established in DOE M 5632.1C-1 and approved by the cognizant DOE element. The vault shall be equipped with intrusion detection alarm protection with protective force response within 30 minutes of alarm annunciation.

(c) In a vault-type room meeting the criteria established in DOE M 5632.1C-1 and approved by the cognizant DOE element. The vault-type-room shall be under intrusion detection alarm protection with protective force response within 30 minutes of alarm annunciation. The vault-type room shall be located within a Limited, Exclusion, Protected, or Material Access Area.

(d) In a vault-type room meeting the criteria established in DOE M 5632.1C-1 and approved by the cognizant DOE element. If located outside of a Limited, Exclusion, Protected, or Material Access Area, the vault-type room shall be under intrusion detection alarm protection with protective force response within 15 minutes of alarm annunciation.

(e) In steel filing cabinets not meeting GSA requirements (such containers approved for use prior to 7-15-94 may continue to be used until October 1, 2012) shall be equipped with three-position, dial-type, built-in changeable combination locks. The cabinet must be within a Limited, Exclusion, Protected, or Material Access Area. In addition, one of the following supplementary controls is required;

1 Intrusion detection alarm protection with protective force response within 30 minutes of alarm annunciation; or

2 Inspection of the container every four hours by protective force.

(3) Confidential Matter. Confidential matter shall be stored in a manner authorized for Secret matter or in a GSA-approved security container.

c. Nonstandard Methods of Storage. Within the minimum protection level of a Limited Area, nonstandard methods of storage may be applied for Top Secret, Secret, and Confidential material whose size, weight, construction, or other characteristics preclude storage as specified in the subparagraphs above.

(1) Local safeguards and security authorities shall base their protection measures upon the results of documented vulnerability analyses. These vulnerability analyses shall address the nature of the matter to be protected (e.g., size, weight, composition, radioactivity, and importance to an adversary and/or the Department) in relation to the threat. Additionally, vulnerability analyses must consider the portability of the classified matter, ease of concealment, time needed to gain access, protective force response time, and the potential consequences of gaining unauthorized access.

(2) Measures (e.g., barriers, locks, intrusion detection systems, and protective force) tailored to address the specific nonstandard condition, as determined by local safeguards and security authority, shall be implemented to provide protection to deter unauthorized access to classified matter.

(3) Measures to be implemented for each nonstandard condition shall be documented in the applicable security plan and approved by the cognizant DOE security office.

(4) For protective force to be employed as a specified supplemental protection measure, due consideration should be given to ensuring the interval for those inspections is less than the time required for an adversary to gain undetected access to the classified matter and/or remove the classified matter and escape detection.

(5) Measures to be implemented for each nonstandard condition shall be documented in the applicable security plan and approved by the cognizant DOE security office. Whenever nonstandard storage methods are implemented, a copy of the vulnerability analysis and description of the protective measures shall be forwarded to the Office of Safeguards and Security and the cognizant program office in Headquarters.

d. Protective Force Personnel. Protective personnel, private security firms, or local law enforcement personnel shall respond to intrusion detection alarms as specified in paragraph 2.b. of this Chapter. Specific details regarding this response (e.g., numbers of protective force personnel responding, response position, duties, etc.) shall be documented in approved security plans.

e. Notification. If an unattended secure storage repository containing classified matter is found open, the repository shall be secured by designated protective personnel and a custodian notified immediately. The contents shall be checked no later than the next workday. If there is an indication of forced entry, compromise, or unaccounted-for matter, the contents shall be checked immediately by a custodian, being careful not to destroy fingerprints or other physical evidence. The incident shall be reported and inquiries conducted as required by Chapter IV of this Manual and DOE O 470.1, SAFEGUARDS AND SECURITY PROGRAM.

f. Alternate Storage Locations.

(1) With prior written approval of the cognizant DOE element, a bank safe deposit box/vault may be used to store Secret or Confidential matter, provided that the lock and keys to the box/vault are changed prior to such use and the customer's key is furnished only to persons authorized access to the contents.

(2) Federal Records Centers, approved as outlined in DOE O 470.1, may be used to store classified information.

3. PROTECTING CONTAINER INFORMATION.

a. Protection of Security Containers and Combinations. The outside of the security container shall 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 shall be kept locked when not under direct supervision of an authorized individual. Combinations shall be protected at the classification level and category of the matter being protected. A minimum number of authorized persons (i.e., personnel having access authorization for the information kept in that container) shall have the combination to the storage container or access to the information stored within the security container.

(1) To ensure proper protection of the combination, part 2 and 2a of each completed SF-700 shall be placed on an envelope and shall be marked with the highest classification level of information authorized for storage in the repository. Part 2a shall be placed inside the envelope and sealed. If the repository reflected on the SF-700 contains RD or FRD, Part 2, and the envelope shall additionally be marked "PROTECT AS RD" or "PROTECT AS FRD" as appropriate. Classifier information is not required to be affixed to part 2 of the SF-700.

(2) Emergency notification personnel or repository custodians with appropriate access authorizations and need to know shall be listed on the SF-700. A record of all persons with knowledge of the combination shall also be maintained. This record may be maintained with the SF-700.

b. Changing Combinations. Combinations shall 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 occurring to an individual knowledgeable of 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;

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

(d) Following maintenance by an uncleared locksmith or safe technician;

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

(3) 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.

(4) Preparation for turn in of the container. The combination shall be set to factory standard 50-25-50 prior to turn-in of the container.

c. Selection of Combination Settings. Combination numbers shall be selected at random, avoiding simple ascending or descending series such as 10-20-30 or 50-40-30. Care shall also 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).

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

(1) Security Container Information. An SF-700, "Security Container Information," shall 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 shall 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," shall be used to record the end-of-day security checks.

(a) The SF-702 shall 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 shall be used in all situations requiring the use of a security container check sheet and shall be affixed to the container or entrance to a room or vault.

(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 shall be maintained according to General Record Schedule 18.

CHAPTER IV

LOSS, POTENTIAL COMPROMISE, OR UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION

1. GENERAL. The loss, potential compromise, or unauthorized disclosure of classified information shall be handled as an incident of security concern according to DOE O 470.1. In addition, the requirements contained in this Chapter apply.

2. RESPONSIBILITY OF DISCOVERER.

   a. Any person observing, finding, or with knowledge of the loss or potential compromise of classified information shall immediately report this information to the facility security officer.

   b. Any person who discovers classified matter out of proper control shall take custody of such matter and safeguard it in an appropriate manner, and shall immediately notify the facility security officer.

3. CLASSIFICATION CONSIDERATION. All discussions and documents associated with the incident shall be handled in accordance with CG-SS-3, "Classification Guide for Safeguards and Security Information," and the classification determination of an authorized classifier.

4. INSPECTION FOR LOST OR UNACCOUNTED-FOR CLASSIFIED MATTER.

   a. Upon determining or learning that classified matter may be lost or unaccounted-for, an inspection of the area(s) where the matter was stored, handled, or processed shall be initiated. The inspection process must be completed within 48 hours.

   b. If the classified matter is found or otherwise accounted for and its safeguarding during the period it was unaccounted for would preclude the possibility of its compromise, the inspection will be discontinued and a determination made as to the cause of the incident. If the incident did not constitute a violation of U.S. law, the categorization, notification, and reporting requirements, set forth below in paragraph 6, are not required.

   c. If the classified matter is either not found, or is found or otherwise accounted for but the safeguarding during the period it was unaccounted for would not preclude the possibility of its potential compromise, the categorization, notification, and reporting requirements, set forth below in paragraph 6, are required.

5. REPORTABLE INCIDENTS.

   a. When loss/compromise has occurred, or the circumstances of the incident cannot rule out the possibility of compromise.

   b. When a violation of U.S. law appears to have occurred.

6. CATEGORIZATION, NOTIFICATION, AND PREPARATION AND SUBMISSION OF UNCLASSIFIED REPORTS.

   a. DOE Elements and contractors at facilities shall develop and maintain implementing procedures for categorizing the incident, notifying DOE, and preparing and submitting reports (initial and updates) for all reportable incidents.

   b. Should the incident meet the criteria as a reportable incident, as set forth above in paragraph 5, reporting of the incident shall be in accordance with DOE Manual 232.1-1A, "Occurrence Reporting and Processing of Operations Information," (ORPS) and via the unclassified ORPS database or otherwise as required by DOE Manual 232.1-1A.

   c. Regarding notifications to DOE, ORPS currently does not require notification/reporting to all organizations with a need-to-know for the information regarding the incident. Therefore, the procedures implemented shall also ensure that notifications (initial and follow-up) are made and that reports (initial and updates) are made available to the following via the unclassified ORPS database or otherwise as required by DOE Manual 232.1-1A:

      (1) The Secretarial Officer(s) with responsibility for the lost, potentially compromised, or compromised classified information.

      (2) The Office of Safeguards and Security if the information lost/compromised or potentially compromised was originated by another Government agency or foreign government.

      (3) The Director of Energy Intelligence if the loss, potential compromise, or unauthorized disclosure involved intelligence-related information.

      (4) The Office of Declassification when the incident involved misclassification or improper declassification by an authorized classifier/declassifier.

   d. Under no circumstances shall classified or UCNI information be entered into the unclassified ORPS database. The transmission in any manner of classified and UCNI information shall be handled in accordance with the requirements of the appropriate security orders.

7. INQUIRY. An inquiry shall be initiated by an appointed Inquiry Official (with previous inquiry experience) within 24 hours of the initial discovery and report of a potential compromise or unauthorized disclosure of classified information, or within 24 hours of the completion of an inspection concerning unaccounted-for classified information.

   a. The inquiry will examine and report all the pertinent facts and circumstances related to the matter under inquiry, which will include but not necessarily be limited to the following:

(1) Determine whether the lost, potentially compromised, or compromised information was properly classified or could be declassified. If an authorized classifier determines that the information is unclassified or can be declassified, the inquiry can be discontinued, however, if the information contained classification markings, all known holders of the information shall be notified so that all copies of the information under government control are declassified and marked accordingly.

(2) If the lost, potentially compromised, or compromised information is determined to be classified, the individuals who may have knowledge regarding the incident shall be interviewed. Upon conclusion of the interview, these individuals may also be requested to provide an official written statement concerning their knowledge of or involvement in the incident.

(3) Complete DOE F 5639.2 (formerly DOE F 5635.11), "Reporting Unaccounted for Documents," or a form comparable in content when classified information is lost or unaccounted-for.

(4) Determine the owner of the lost/compromised or potentially compromised information (i.e., the DOE Secretarial Officer with programmatic responsibility for the information or whether the information was originated by another Government agency or foreign government).

(5) Determine whether loss/compromise did or did not occur, the probability of compromise is remote, or the probability of compromise is not remote. The basis for such findings must be documented.

(6) If loss/compromise has occurred or the circumstances of the incident cannot rule out the possibility of compromise, establish the extent of the dissemination of the classified information and ensure that appropriate measures (e.g., sanitizing electronic media) are taken to mitigate the loss, potential compromise, or unauthorized disclosure.

(7) Determine the cause(s) of the incident, to include root, direct, and contributing causes as required by DOE Manual 232-1-1A.

(8) Determine the individual(s) responsible for the incident.

(9) Determine whether the incident involves an inadvertent or deliberate failure to follow DOE safeguards and security regulations and directives, a statute, Executive Order, and/or a national directive that does not constitute a crime, or a violation of U.S. laws or their implementing regulations. Ensure that all violations of U.S. laws applicable to the matter under inquiry are identified. When an inquiry establishes credible information that a violation of U.S. law pertaining to the unauthorized disclosure of classified information has occurred, the Department of Justice (DOJ) Eleven-point Criteria must be completed. The completion of the DOJ Eleven-point Criteria is not required for any other violations of U.S. law (i.e., except unauthorized disclosures). When completing the DOJ Eleven-point Criteria, all

documentation and appropriate information must be provided to support affirmative responses to the 11 criteria (i.e., questions) listed below. In addition, each question must be answered affirmatively for DOJ to initiate a formal investigation into the unauthorized disclosure. However, a failure to affirmatively answer all criteria of the DOJ 11 points does not preclude DOE from pursuing criminal action for an unauthorized disclosure.

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

(b) Could specific statements in the article which 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 the individual(s) responsible for the security of the classified data disclosed?

(e) Could the extent and 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 which 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?

(10) Estimate the known or probable damage to the national security that has resulted or may result for all reportable occurrences.

(11) Determine the corrective action(s) to be taken to prevent recurrence.

(12) Document the findings of the inquiry (i.e., the facts and circumstances related to the matter under inquiry) in a written report. The Reports shall include the facility name and facility code (as registered in DOE's Safeguards and Security Information Management System) or other identification as appropriate for the facility responsible for the incident, and the facility where the incident occurred.

(a) If the inquiry determines that the facts of the incident rule out the possibility of compromise and in addition the incident did not constitute a violation of U.S. criminal laws, the Inquiry Official is not required to produce a formal Report of Inquiry. The DOE Form 5639.3, "Report of Security Incident/Infraction," or a form comparable in content, can be used for documenting such incidents, to include corrective action taken to prevent recurrence.

(b) If the inquiry determines that loss/compromise has occurred, the circumstances of the incident cannot rule out the possibility of compromise, and/or a violation of criminal law appears to have occurred, the facts and circumstances related to the matter under inquiry shall be documented in a written official Report of Inquiry. Attachments to the Report of Inquiry shall include the Memorandum of Appointment of the Inquiry Official, any signed statements of involved individuals, a copy of the lost/compromised or potentially compromised information or a description of same (as appropriate), completed DOE Form 5639.3, a copy of the final ORPS occurrence report for the incident, and any other information important to the inquiry.

b. At a minimum, the following distribution shall be made upon completion of the reports. If there is any significant change or new information about the incident, to include the status of criminal prosecutions, update reports identifying the incident and providing the new information shall also be distributed in a prompt manner to the following:

(1) A copy of the DOE Form 5639.3, or a form comparable in content, shall be forwarded through the cognizant DOE safeguards and security organization, to the Office of Safeguards and Security.

(2) A copy of the written official Report of Inquiry, with supporting statements/documentation, shall be forwarded, through the cognizant DOE safeguards and security organization, to the Office of Safeguards and Security and the Secretarial Officer with programmatic responsibility for the lost, potentially compromised, or compromised classified information.

8. DISCIPLINARY ACTIONS AND CORRECTIVE MEASURES. Upon completion of the inquiry, the cognizant DOE safeguards and security organization shall ensure:

a. The party(ies) responsible for the loss, potential compromise, or unauthorized disclosure of classified information are identified and punished appropriately. The appropriate administrative, disciplinary, or other adverse action may be taken at any time for DOE and contractor employees. However, whenever a criminal violation appears to have occurred and a criminal prosecution is contemplated against a DOE and/or contractor

employee(s) believed responsible for the loss/compromise of classified information, such disciplinary action will be coordinated with the appropriate investigative or prosecuting officials to avoid prejudice to any criminal investigation or prosecution.

b. Whenever a criminal violation appears to have occurred and a criminal prosecution is contemplated against any person(s) believed responsible for the loss/compromise of classified information, the cognizant DOE safeguards and security organization responsible for the inquiry shall apprise the legal counsel of the Departmental Element (i.e., Office of the General Counsel or Chief Counsel Office) where the individual(s) responsible is assigned or employed.

c. Corrective actions are taken to preclude recurrence of conditions or activities that allowed or contributed to the loss, potential compromise, or unauthorized disclosure of classified information.

9. DAMAGE ASSESSMENTS.

a. Purpose. Damage assessments are used by the Department of Justice when criminal prosecution is sought, by responsible managers to determine future courses of action within the program, and by security personnel for evaluating possible countermeasures and document actions to limit potential damage.

b. When Required.

(1) Whenever the inquiries disclose evidence that classified information has been compromised and the compromise can reasonably be expected to cause damage to the national security, a damage assessment is required.

(2) Whenever a violation of criminal law(s) appears to have occurred and a criminal prosecution is contemplated, a damage assessment is required..

(3) Whenever the inquiries disclose evidence that classified information may have been compromised (i.e., the circumstances of the incident cannot confirm compromise, however, the possibility of compromise cannot be ruled out), and the compromise of this classified information could be expected to cause damage to the national security, the Secretarial Officer with programmatic responsibility for the potentially compromised classified information must determine whether a damage assessment is required. This determination shall be based on the circumstances of the loss/compromise and the sensitivity of the information.

c. Conduct of Damage Assessment. The Secretarial Officer with programmatic responsibility for the compromised or potentially-compromised classified information shall appoint a Federal 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 and/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 or potentially-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 team performing the damage assessment shall prepare a draft assessment and coordinate it with the originator of the compromised or potentially-compromised information.

(3) The damage assessment shall then be approved by the Secretarial Officer with programmatic responsibility for the compromised or potentially-compromised information and, at a minimum, submitted to the Office of Safeguards and Security, the Office of Declassification, and the cognizant DOE safeguards and security organization responsible for the inquiry.

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

e. Content of a Damage Assessment Report. At a minimum, damage assessment reports shall contain the following:

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

(2) Classification of the specific information compromised or potentially compromised.

(3) Description of the specific information compromised or potentially compromised.

(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 governments and/or hostile organizations resulting from the compromise or potential compromise.

(6) An assessment and recommendation to the Office of Declassification as to whether classification of the information should be continued without change; specific information, or parts thereof, shall be modified to minimize or nullify the effects of the reported loss/compromise and the classification retained; and downgrading, declassification, or upgrading is warranted.

(7) An assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise or potential 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 loss, potential compromise, or unauthorized disclosure of classified information, damage assessments shall be coordinated with the legal counsel of the DOE Element (i.e., Office of the General Counsel or Chief Counsel Office) where the individual responsible is assigned or employed.

g. Combining Similar Documents. Damage assessments may be completed for a group of similar incidents when such 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 the same or similar damage to the national security or advantage to foreign governments and/or hostile organizations.

h. Cases Involving Other Government Agency Information. Whenever a compromise or potential compromise involves the classified information of another Government agency, the cognizant DOE safeguards and security organization responsible for the inquiry shall provide, through the Office of Safeguards and Security, the circumstances and findings that affect the other government agency's information or interests.

i. Cases Involving Foreign Government Information. Whenever a compromise or potential compromise involves the classified information of a foreign government, the cognizant DOE safeguards and security organization responsible for the inquiry shall provide, through the Office of Safeguards and Security, the circumstances and findings that affect the foreign government's information or interests, however, the foreign government shall not normally be advised of any DOE security system vulnerability(ies) that allowed or contributed to the compromise or potential compromise.

j. Joint Damage Assessment with Another Government Agency. Whenever a compromise or possible compromise involves the classified information or interests of more than one government agency, the following conditions apply:

(1) Another government agency has the inherent responsibility to conduct the damage assessment on their compromised or potentially compromised information.

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

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

(4) Whenever a compromise or potential 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 Safeguards and Security shall ensure, through appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained.

(5) Whenever a compromise or potential compromise of Sensitive Compartmented Information has occurred, the Director 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.

10. SYSTEM OF CONTROL. DOE Elements and contractors at facilities shall establish a system of controls and procedures to ensure that inquiries and damage assessments are conducted when required, that all information pertinent to the matter under inquiry is maintained in the official file for the incident, and that those records are maintained in a manner that facilitates their retrieval and use.

11. RECORDS RETENTION. Records pertaining to the loss, potential compromise, or unauthorized disclosure of classified information shall be destroyed 5 years after the close of all associated actions. These records shall not be sent to Federal Records Centers.

CONTRACTOR REQUIREMENTS DOCUMENT

PROTECTION AND CONTROL OF CLASSIFIED MATTER

This contractor requirements document is issued to aid in the identification of requirements applicable to contractors. All requirements contained in Manual 471.2-1B apply to contractors with access to classified matter. The requirements in this Manual shall flow down to all subcontractors with access to classified matter.